



Coordinated Security & Privacy Disclosure, Final Report

Runna for Android (com.runbuddy.prod)

A Sentry organization auth token shipped inside a running app with heart-rate access,
silently removed in October without a word to the reporter, revocation still unconfirmed

**PUBLIC DISCLOSURE, 26 OCTOBER 2026 – EMBARGO ENDED 22 OCTOBER
2026, ZERO REPLIES, TOKEN SILENTLY REMOVED IN 8.59.0**

Target	The Run Buddy Limited, trading as Runna, London, United Kingdom. Google Play developer of record: Strava, Inc.
Product audited	Runna for Android, com.runbuddy.prod, production APK installed on the RFI-IRFOS test device on 22 June 2026
Disclosure reference	REF RUNNA-2026-R1
First notice	2026-06-22 (privacy@runna.com, bounced)
Notice at a working address	2026-07-23 (dpo@runna.com, cc EU representative)
Re-verification	2026-10-26, Runna 8.59.0 (versionCode 2084), pulled from Google Play onto the RFI-IRFOS test device
Disclosure / embargo date	2026-10-22
Report published	2026-10-26
Severity	CRITICAL (C1 Sentry organization auth token, CVSS v4.0 8.7, RFI-IRFOS blast-radius escalation, see C1). C1 removed from 8.59.0, revocation unconfirmed

security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1	Executive Summary	4
2	Subject & Operator Analysis	6
3	Positive Observations	6
4	Findings	6
4.1	C1: Sentry organization auth token hardcoded in the production APK. RE-MOVED IN 8.59.0, REVOCATION UNCONFIRMED	6
4.2	C2: Production Firebase configuration hardcoded	7
4.3	C3: Advertising attribution SDK inside a health app, absent from the privacy policy	7
4.4	C4: Meta App Events and a hardcoded Facebook client token	8
4.5	C5: Two Mixpanel analytics projects, one for watchOS, absent from the privacy policy	8
4.6	H1: Cleartext traffic permitted, no network security configuration	8
4.7	H2: Sentry native layer preloads at the highest init priority	9
4.8	H3: RECORD_AUDIO declared without a documented purpose	9
4.9	NG1: New in 8.59.0 review: Consent Mode defaults granted for advertising, no consent platform	9
5	Impact Analysis	10
6	The Complete Chain	10
7	Regulatory Framework	10
8	Indicators of Compromise	11
9	Data Protection, Article by Article	11
10	Questions Left Unanswered	12
11	Disclosure Timeline	12
12	Residual Risk	13

Executive Summary

On 22 June 2026, RFI-IRFOS performed static analysis of the production Runna Android application. Runna is an AI running coach. It reads heart rate, exercise sessions, steps, calories, speed and elevation through Android Health Connect, and it records GPS routes. Heart rate is health data under GDPR Art. 9(1).

The most significant finding is a Sentry organization auth token for the organization "runna", hardcoded in `res/values/strings.xml`. A Sentry DSN only lets an app send crash reports. An auth token, prefix `sntrys_`, authenticates against the Sentry API itself. Anyone who unpacks the APK holds it. RFI-IRFOS did not use the token and did not test its scope.

On 26 October 2026, four days after the embargo ended, RFI-IRFOS pulled the current build, 8.59.0. The Sentry auth token is gone. `SENTRY_WATCH_AUTH_TOKEN` has been replaced by `SENTRY_WATCH_DSN`, and the prefix `sntrys_` appears nowhere in the resources or the dex code. Runna therefore acted on the finding, and told nobody. Removal from a new build does not invalidate the token held by every older copy of the app. Whether the token was revoked in Sentry is known only to Runna. Every other finding persists unchanged in 8.59.0.

Five further credentials ship in the same file: a Firebase API key for the production project `rb-app-prod`, an AppsFlyer dev key, a Facebook client token, and two Mixpanel project tokens, one of them labelled for watchOS.

8.59.0 also declares all four Google Consent Mode defaults as granted in its manifest, including ad storage, ad user data and ad personalization, and enables advertising ID collection. No consent management platform ships in the build. In a health app whose privacy policy promises to keep heart rate out of advertising, the advertising signals are switched on before the user has been asked anything (NG1).

Runna's privacy policy promises that heart rate and other health information from connected devices will not be used for advertising and will not be disclosed to third parties without prior consent. The same binary that reads heart rate ships an advertising attribution SDK (AppsFlyer, 481 classes), Meta's App Events and two Mixpanel analytics projects. The policy names Meta in general terms as an advertising publisher. It does not name AppsFlyer, Mixpanel or Sentry at all. Static analysis shows these SDKs sit inside the health app. It does not show which event fields they transmit, and this report does not claim it does.

RFI-IRFOS sent four notices to the working DPO address over 91 days. Runna never replied, not even with an automated acknowledgment. World context, queried 26 October 2026 against CISA KEV, NVD and our DINGIR feed: no actively exploited vulnerability names Runna. Two new Sentry CVEs appeared in the window (CVE-2026-114139 in the JavaScript SDK, CVE-2026-102899 in Sentry's SAML SSO), neither is shown to affect this app.

Scope: Static analysis of the production Runna Android APK, installed from Google Play on an RFI-IRFOS test device, re-verified on 26 October 2026 against the current Play Store build 8.59.0 (versionCode 2084, base APK SHA-256 467ef70774a20096706f31a427791dcb352a69a298f37900596a83ab799a38ba), plus a reading of Runna's published privacy policy on 26 October 2026. No Runna account, backend, Sentry organization or third-party service was accessed or tested. None of the credentials named in this report was used.

Disposition

The original notice of 22 June 2026 went to privacy@runna.com, which bounced permanently. RFI-IRFOS located the data protection officer address in Runna's own privacy policy and resent the full disclosure to dpo@runna.com on 23 July 2026, cc the EU GDPR representative (Instant EU GDPR Representative Ltd., contact@gdprlocal.com) and the Austrian DSB. Follow-ups went to the same address on 15 August, 12 September and 17 October 2026. None of the four bounced. None was answered.

ID	Severity	Title
C1	CRITICAL	Sentry organization auth token hardcoded in the production APK. REMOVED IN 8.59.0, REVOCATION UNCONFIRMED
C2	MEDIUM	Production Firebase configuration hardcoded
C3	HIGH	Advertising attribution SDK inside a health app, absent from the privacy policy
C4	HIGH	Meta App Events and a hardcoded Facebook client token
C5	MEDIUM	Two Mixpanel analytics projects, one for watchOS, absent from the privacy policy
H1	MEDIUM	Cleartext traffic permitted, no network security configuration
H2	MEDIUM	Sentry native layer preloads at the highest init priority
H3	LOW	RECORD_AUDIO declared without a documented purpose
NG1	MEDIUM	New in 8.59.0 review: Consent Mode defaults granted for advertising, no consent platform

Subject & Operator Analysis

Runna was founded in London as RunBuddy, which is why the Android package is still com.runbuddy.prod. The privacy policy names The Run Buddy Limited as controller, dpo@runna.com as data protection contact, and Instant EU GDPR Representative Ltd. as EU representative. Google Play lists Strava, Inc. as the developer. Runna is a separate company from runna GmbH, the Swiss operator of running.COACH.

Positive Observations

allowBackup is false, so Health Connect data is not copied into Google cloud backups. Health Connect permissions are declared correctly and Android asks the user at runtime. We swept for Chinese SDKs (Tencent, ByteDance, Huawei) and found none. We found no biometric identity SDK.

Findings

C1: Sentry organization auth token hardcoded in the production APK. REMOVED IN 8.59.0, REVOCATION UNCONFIRMED

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7 (CVSS-B), escalated to CRITICAL, see text

A Sentry auth token for the organization "runna" is stored in res/values/strings.xml under the name SENTRY_WATCH_AUTH_TOKEN. Its decoded header names the organization and the US Sentry region. A DSN only accepts events. An auth token is an API credential. RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because the credential belongs to the whole Sentry organization rather than to one client, and in a running app with heart-rate access the stored error events, breadcrumbs and any session replays are the data most likely to carry health and location context. We did not call the Sentry API, so the token's exact scopes remain untested.

```
SENTRY_WATCH_AUTH_TOKEN = sntrys_[REDACTED]
Decoded header: {"iat":1698230432,"url":"https://sentry.io","region_url":"https://us.sentry.io","org":"runna"}
Issued (iat):    25 October 2023
```

The issue date in the header means the token was minted in October 2023. It was still shipping in June 2026. Rotation is the only fix. Removing it from the next build leaves every installed copy holding a live credential until the token is revoked.

```
8.59.0, 26 Oct 2026
SENTRY_WATCH_AUTH_TOKEN: absent
sntrys_ anywhere:       0 hits (res/, classes*.dex)
SENTRY_WATCH_DSN:       https://[REDACTED]@o512760.ingest.sentry.io/4506110496145408
```

The token is gone from 8.59.0 and a DSN took its place, which is the correct construction for a watch client that only sends events. The change shipped without a reply to any of the four notices. RFI-IRFOS cannot see whether the token was revoked. Until Runna confirms revocation, every earlier build of the app, on phones and on APK mirror sites, still carries a credential that may work.

C2: Production Firebase configuration hardcoded

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9

The Firebase API key, app ID and project ID of the production project ship in the binary. Firebase keys are designed to be public identifiers, so the risk depends on the project's security rules and API restrictions, which we did not test. The ID C2 is kept from the original notice. The severity is scored under CVSS v4.0 for publication.

```
google_api_key = AIzaSyAwyzj0UZ739r0f-rJ2zKY2HJT4GhTckzA
google_app_id  = 1:942402709455:android:elc294ae27038de61f94ba
project_id     = rb-app-prod
```

C3: Advertising attribution SDK inside a health app, absent from the privacy policy

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N, 7.7

AppsFlyer ships with 481 classes and a hardcoded dev key. AppsFlyer links installs and in-app events to the advertising campaign that produced them and to the device advertising ID. The privacy policy does not name AppsFlyer. The app's backup rules file is named `appsflyer_backup_rules.xml`: the attribution data gets its own backup exclusion.

```
AF_DEV_KEY = JMqd9jupV72puqLJueZzBF
AppsFlyer smali classes: 481
res/xml/appsflyer_backup_rules.xml
```

What a runner experiences: the app that knows their heart rate zones and when they train also reports their use of the app to an attribution network that works for advertisers. Runna's own policy promises health data stays out of advertising. Which in-app events the SDK carries is set at runtime, and RFI-IRFOS did not observe them.

C4: Meta App Events and a hardcoded Facebook client token**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N, 7.7**

The Facebook SDK's App Events module (11 classes) ships with a hardcoded client token, stored twice. App Events delivers in-app behaviour to Meta's advertising systems. The privacy policy names Meta only as a publisher that places Runna's ads. It does not say that the app itself reports in-app events to Meta.

```
FACEBOOK_CLIENT_TOKEN = 7ca38529e526bf234dd8913cbde77ec7 (stored twice)
com/facebook/appevents smali classes: 11
```

C5: Two Mixpanel analytics projects, one for watchOS, absent from the privacy policy**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9**

Two Mixpanel project tokens ship in the Android build, one named for the Android app and one for watchOS. Mixpanel is a US analytics provider. The privacy policy does not name it, so a user cannot see that a US processor receives product analytics from a running and heart-rate app (GDPR Art. 13(1)(e), Art. 46).

```
MIXPANEL_PROJECT_TOKEN = c6d87010db04ac3b957a2057cdc4d8ec
MIXPANEL_WATCHOS_PROJECT_TOKEN = 717440d67e7d113861f45e1541f5f4dc
Mixpanel smali classes: 33
```

H1: Cleartext traffic permitted, no network security configuration**MEDIUM, CVSS v4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 6.0**

The manifest sets `usesCleartextTraffic="true"` and declares no `networkSecurityConfig`. Plain HTTP is therefore allowed for every host the app contacts, and there is no certificate pinning. Whether any production endpoint actually uses HTTP was not tested.

H2: Sentry native layer preloads at the highest init priority**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1**

io.sentry.auto-init is set to false, yet io.sentry.ndk.SentryNdkPreloadProvider is registered with initOrder=2000000000, the highest value Android allows. It loads the native Sentry layer before any app code, and so before any consent decision. Sentry ships with 1,240 classes.

H3: RECORD_AUDIO declared without a documented purpose**LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0**

The app declares RECORD_AUDIO. Android asks the user before granting it, so this is not silent recording. The privacy policy names no purpose, processor or legal basis for audio (GDPR Art. 5(1)(c), Art. 13).

NG1: New in 8.59.0 review: Consent Mode defaults granted for advertising, no consent platform**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 6.9**

The manifest of 8.59.0 sets google_analytics_default_allow_analytics_storage, _ad_storage, _ad_user_data and _ad_personalization_signals to true, sets firebase_analytics_collection_enabled and google_analytics_adid_collection_enabled to true, and declares the AD_ID permission. No consent management platform (Usercentrics, OneTrust, Didomi, Google UMP) ships in the build. The Firebase and AppsFlyer consent methods exist as SDK APIs. Static analysis cannot show whether Runna calls them after a dialog of its own. Until such a call happens, Google treats consent for advertising as given.

```
<meta-data android:name="google_analytics_default_allow_analytics_storage" android:
  value="true"/>
<meta-data android:name="google_analytics_default_allow_ad_storage" android:value="
  true"/>
<meta-data android:name="google_analytics_default_allow_ad_user_data" android:value="
  true"/>
<meta-data android:name="google_analytics_default_allow_ad_personalization_signals"
  android:value="true"/>
<meta-data android:name="google_analytics_adid_collection_enabled" android:value="true
"/>
```

Consent Mode v2 exists so that apps declare these signals as denied until the user decides. Declaring them granted is the opposite configuration. Under § 165(3) TKG 2021, § 25 TDDDG and GDPR Art. 6(1)(a), storing and reading the advertising ID and passing ad user data to Google requires prior consent. The privacy policy says health information is never used for advertising. The same build hands Google advertising signals by default. Whether those signals carry health events is not visible statically, and that question goes to Runna.

Fix: Set the four `google_analytics_default_allow_*` keys and `adid_collection_enabled` to false, ask for consent through a CMP, and call `setConsent` with the user's decision.

Impact Analysis

Who is affected: people who train with Runna, many of them preparing for a first race or a marathon, who connect a watch or chest strap and let the app read heart rate in Health Connect. Runna sells a paid subscription. So the usual defence that the user pays with data does not apply here: these users pay with money and the app still carries an ad attribution SDK, Meta App Events and two analytics projects.

What the Sentry token means in practice: crash and error reports of a fitness app routinely carry device model, app state, screen names, breadcrumbs of the last user actions and, with session replay enabled, a recording of the screen. An organization-level read credential turns that store into something anyone with apktool can query. We did not test whether replay is enabled or which scopes the token holds.

The Complete Chain

Google Play install, every Android user of Runna → one APK, `com.runbuddy.prod` → `res/values/strings.xml` holds six credentials in plain text → one of them, `sntrys_`, is an API credential for the Sentry organization "runna" on the US region, issued October 2023 → the same APK reads heart rate and exercise sessions from Health Connect and ships AppsFlyer, Meta App Events and Mixpanel → the privacy policy promises health data stays out of advertising and names none of AppsFlyer, Mixpanel or Sentry → four notices to the DPO in 91 days, zero replies.

26 October 2026, build 8.59.0: the token is gone and a DSN replaced it. Nobody at Runna said so. Revocation is unconfirmed. In the same build, Google's advertising consent is set to granted by default.

Regulatory Framework

Runna is a UK company with an EU representative under GDPR Art. 27, so the EU GDPR applies to its EU users and UK GDPR to its UK users. Heart rate is health data under Art. 9(1). Art. 32 requires security appropriate to that risk, and a shipped API credential falls below it. Art. 13(1)(e) requires the recipients to be named. Transfers to US processors need a basis under Art. 44 to 46. The Austrian DSB was copied on the disclosure from 23 July 2026. The UK ICO's casework address rejected the original notice through a mail rule.

Indicators of Compromise

Indicator	Where	Meaning
sntrys_token, org runna, iat 1698230432	res/values/strings.xml, SENTRY_WATCH_AUTH_TOKEN	Sentry API credential, absent from 8.59.0. Still present in every earlier build until revoked
rb-app-prod / AlzaSyAwYzj0UZ739rOf-rJ2zKY2HJT4GhTckzA	strings.xml google_api_key	Production Firebase project
JMqd9jupV72puqLJueZzBF	AF_DEV_KEY	AppsFlyer dev key
7ca38529e526bf234dd8913cbde77ec7	FACEBOOK_CLIENT_TOKEN	Meta client token
c6d87010db04ac3b957a2057cdc4d8ec, 717440d67e7d113861f45e1541f5f4dc	MIXPANEL_*_PROJECT_TOKEN	Mixpanel Android and watchOS projects
initOrder=2000000000	io.sentry.ndk.SentryNdkPreloadProvider	Native SDK preload before app code
google_analytics_default_allow_* = true	AndroidManifest.xml, 8.59.0	Advertising consent granted by default (NG1)

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	API credential for the whole Sentry organization in a public binary
C2	GDPR Art. 32(1)	Production Firebase configuration in the binary
C3	GDPR Art. 9(2), Art. 13(1)(e)	Ad attribution SDK in a health app, not named in the privacy policy
C4	GDPR Art. 13(1)(e), Art. 6(1)	In-app events to Meta, not disclosed as such
C5	GDPR Art. 13(1)(e), Art. 46	US analytics processor not named
H1	GDPR Art. 32(1)(a)	Cleartext allowed app-wide
H2	GDPR Art. 25(2)	Native SDK layer starts before any consent decision
H3	GDPR Art. 5(1)(c), Art. 13	Audio permission without a stated purpose

Questions Left Unanswered

1. Has the Sentry auth token been rotated, and which technical measure under Art. 32(1)(a) now prevents auth tokens from shipping in production builds?
2. Is a DPO or privacy-responsible person aware of this finding?
3. Is there a documented risk assessment covering the other five hardcoded credentials?

Disclosure Timeline

Date	To	Result
2026-06-22	privacy@runna.com	Bounced permanently (550 5.1.1)
2026-07-23	dpo@runna.com, cc contact@gdpr local.com, DSB	Delivered, no reply
2026-08-15	dpo@runna.com, cc contact@gdpr local.com, DSB	Delivered, no reply
2026-09-12	dpo@runna.com, cc contact@gdpr local.com, DSB	Delivered, no reply
2026-10-17	dpo@runna.com, cc contact@gdpr local.com	Delivered, no reply
2026-10-26	Re-verification of 8.59.0	Token removed silently, revocation unconfirmed. NG1 found. Report published

Residual Risk

Runna removed the Sentry auth token from 8.59.0. Removal does not revoke it. Every copy of an earlier build on a phone or an APK mirror still carries the token, and it keeps working until Runna revokes it in Sentry. Runna has not said whether that happened.

The gap between the privacy policy and the binary stays open until the policy names every processor that ships in the app, or the SDKs leave the health app. Runna's own promise that heart rate stays out of advertising is checkable only if the company states which events reach AppsFlyer, Meta and Mixpanel.

The Consent Mode defaults in 8.59.0 (NG1) send advertising signals before any choice. That stays open until the defaults are set to denied and a consent dialog decides.

RFI-IRFOS keeps pulling the Runna APK and compares builds by SHA-256. A silent rotation or removal will be added to this record, in the same way as any new finding.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 9, 13, 25, 32, 46. REF RUNNA-2026-R1.