Coordinated Privacy Disclosure, Final Report

running.COACH (me.runningcoach)

runna GmbH / running.COACH, a Swiss-regulated AI running-coaching platform (runningcoach.me)

SILENT · CASE CLOSED AND PUBLISHED 24 SEPTEMBER 2026, 95 DAYS AFTER DISCLOSURE, MULTIPLE CHANNELS TRIED, ZERO REPLY OF ANY KIND

Target	running.COACH, an AI-driven running training-plan app connecting to Health Connect heart-rate and exercise data
Package	me.runningcoach
Operator	runna GmbH / running.COACH (runningcoach.me), Swiss-regulated (nDSG), also subject to GDPR for EU users
Initial Disclosure	2026-06-22
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-24, five days after the embargo, an internal publishing gap, not a change in terms
Regulators in BCC/CC	Austrian DSB, CERT.at, Swiss FDPIC (info@edoeb.admin.ch), UK ICO (attempted, blocked by a mail-flow rule)
Total Outbound Messages	10+ across three parallel channels (info@runningcoach.me, running.coach@quevita.zendesk.com, dpo@runna.com) over 95 days, after the initial attempt via casework@ico.org.uk was blocked by a recipient-side mail rule.
Inbound Replies	0. No reply, automated or human, was ever received on any of the three channels tried.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 22 June 2026, RFI-IRFOS disclosed to running.COACH that its own privacy policy states plainly, in these words, that "no user data is shared with independent third parties," while the production Android binary ships Huawei Mobile Services activity-recognition tracking, 1,136 Sentry session-instrumentation classes, and an Android Auto Backup configuration that transmits every training session, every heart-rate measurement, and every planned workout to Google Cloud, with backup-exclusion rules written narrowly enough to exclude only a GPS SDK's own configuration files, not any of the user's actual health data.

The most serious finding is architectural, not a single credential: running.COACH ships with no Network Security Configuration file at all, meaning the app falls back to Android's platform defaults, certificate pinning is entirely absent, and cleartext traffic remains permitted on any device running an Android version below 9. Health Connect heart-rate and exercise data, the app's core product, travels over this configuration on every training session, in whatever network context a runner happens to be in.

RFI-IRFOS attempted contact through three separate, parallel channels over 95 days: info@runningcoach.me directly (cc running.coach@quevita.zendesk.com), dpo@runna.com (a data-protection contact for the shared developer organization), and an initial attempt to casework@ico.org.uk that was blocked outright by a recipient-side Microsoft 365 mail-flow rule before it ever reached its destination. Ten or more messages were sent in total, cc'ing the Austrian DSB, CERT.at, and the Swiss FDPIC throughout. Not one reply, automated or human, was ever received on any channel. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish five days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production running.COACH Android application (me.runningcoach), covering the AndroidManifest, network security configuration (or its absence), resource strings, and decompiled dex/smali, as pulled and reviewed on 22 June 2026. No dynamic instrumentation, live traffic capture, or interaction with running.COACH's backend infrastructure was performed. A related but distinct correspondence thread concerning a sibling application under the same developer organization, involving a separate credential-exposure finding, is tracked independently and is not included in this report's scope or scoring.

Disposition

Five findings were disclosed on 22 June 2026, later re-scored under CVSS v4.0. One finding is held at CRITICAL under an explicit, stated blast-radius escalation: the app ships with no Network Security Configuration at all, meaning real-time heart-rate and exercise data from Health Connect travels with no certificate pinning and no cleartext restriction, on an application whose realistic use context, gyms, races, public running routes, involves connecting to unfamiliar or shared networks. Two further findings, a hardcoded Firebase key and undisclosed Huawei HMS/Sentry data recipients contradicting the app's own privacy policy, correct down to MEDIUM. A backup-exposure finding corrects down to LOW. Ten or more messages were sent across three separate contact channels over 95 days. Not one reply of any kind was ever received on any of them.

ID	Severity	Title
C1	LOW	allowBackup=true With No Exclusion for Health or Training Data, Contradicting the App's Own "No Third-Party Sharing" Policy
C2	MEDIUM	Firebase API Key Hardcoded in the Distributed Binary
H1	CRITICAL	No Network Security Configuration at All: Real-Time Heart-Rate and Exercise Data Travels With No Certificate Pinning and No Cleartext Restriction
H2	MEDIUM	Huawei HMS Activity Recognition, an Undisclosed PRC-Subject Data Recipient
H3	MEDIUM	Sentry, 1,136 Classes With Registered Content-Providers, Plus Background Health-Data Reads, Neither Disclosed

Subject & Operator Analysis

running.COACH (me.runningcoach) is an AI-driven running training-plan app, connecting to Android Health Connect for heart-rate and exercise data, operated under Swiss data protection law (nDSG) with GDPR applying to EU users. Its own privacy policy states plainly that no user data is shared with independent third parties, a claim this audit set out to test against the production binary, not the policy text.

Several genuine positives are worth naming. No Facebook SDK, no MoEngage or Braze marketing-automation platform, and no biometric SDK were found in the binary. Health Connect permissions are runtime-granted, requiring explicit user consent at the OS level. The core training-plan product itself is technically well-built; the issues documented here sit in the data-infrastructure layer around it, not in the product's central functionality.

Three Channels, Ten Messages, Zero Reply

This case's correspondence record spans three separate channels because the first two did not work. An initial attempt via casework@ico.org.uk was blocked outright by a Microsoft 365 mail-flow rule at the recipient's domain before it could ever be read. RFI-IRFOS then pursued info@runningcoach.me directly, cc'ing the shared developer organization's Zendesk queue (running.coach@quevita.zendesk.com), and separately dpo@runna.com. Ten or more messages were sent across these channels over 95 days, cc'ing the Austrian DSB, CERT.at, and the Swiss FDPIC throughout. Not one reply, automated or human, was ever received on any of them.

Findings

C1: allowBackup=true With No Exclusion for Health or Training Data, Contradicting the App's Own "No Third-Party Sharing" Policy

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4.

android:allowBackup="true" is set, and the app's backup-exclusion rules exclude only a GPS tracking SDK's own configuration files, not any of the user's actual data. Every completed training session, every heart-rate measurement, and every planned workout is backed up to Google Cloud via Android Backup Service, unexcluded. running.COACH's own privacy policy states that personal data is used solely for registration-required services and is not shared with independent third parties; Google LLC, as the backup-service processor, is such a third party and is not named in that policy. Exploiting this exposure requires local device access or a compromised Google account and backup-extraction path, which is why this corrects down from the original CRITICAL label; the underlying policy-contradiction and health-data-scope gap remain real.

```
android:allowBackup="true"
backup_rules.xml excludes:
  <exclude domain="sharedpref" path="TSLocationManager.xml" />
  <exclude domain="sharedpref" path="TSLocationManager:TSConfig.xml" />
# excluded: GPS SDK's own config. NOT excluded: training plans, session
# history, heart rate data, planned workouts, user preferences.
```

Impact: A party with local device access, or a compromised Google account with backup access, could recover a user's full training and heart-rate history, data the app's own privacy policy says is not shared with any third party, including its own backup infrastructure provider.

Fix: Extend the backup-exclusion rules to cover training history, session data, and Health Connect-derived data, or disable allowBackup for health-data-bearing storage paths specifically. No confirmation that this has occurred was ever received.

C2: Firebase API Key Hardcoded in the Distributed Binary

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

The Firebase API key, app ID, and project ID (rc-cross) are present verbatim in res/values/strings.xml, extractable from the public APK in under a minute. Firebase keys are not secrets by design, so this finding concerns availability, not confidentiality: a party holding the key can attempt database enumeration, Remote Config tampering, and Cloud Messaging spoofing against the rc-cross project.

```
res/values/strings.xml
google_api_key  = AIzaSyDMqTMMEg-9Z9Vje-VJhIJrNZUCDRsw0tk
google_app_id   = 1:997181887843:android:6708a010a03d361cd12f56
project_id      = rc-cross
```

Impact: A party holding the exposed credential could attempt to enumerate or tamper with the rc-cross Firebase project's Remote Config and Cloud Messaging configuration, potentially affecting service behavior for all users.

Fix: Rotate the exposed key, apply Firebase App Check and key restrictions, and route sensitive configuration through an authenticated backend layer. No confirmation that this has occurred was ever received.

H1: No Network Security Configuration at All: Real-Time Heart-Rate and Exercise Data Travels With No Certificate Pinning and No Cleartext Restriction

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 7.1. RFI-IRFOS blast-radius escalation: raised from HIGH/7.1 to CRITICAL because a running app is realistically used on unfamiliar and shared networks, gyms, race-day WiFi, public routes, and this finding means the app's real-time Art. 9 health data, heart rate above all, has zero technical protection against interception in exactly those contexts.

No network_security_config attribute is declared anywhere in the AndroidManifest, meaning the app falls back entirely to Android's platform defaults: system CAs only, no certificate pinning, and cleartext traffic permitted on any device running Android below version 9. Health Connect heart-rate streams, exercise session uploads, pace, distance, and elevation data all travel under this unprotected configuration. A person on an attacker-controlled or compromised network, a rogue access point at a gym, a race expo, or a public running trailhead, is positioned to intercept or manipulate this traffic. RFI-IRFOS blast-radius escalation: raised from HIGH/7.1 to CRITICAL because a running app is realistically used on unfamiliar and shared networks, and this finding means real-time Art. 9 health data has zero technical protection against interception in exactly those contexts.

```
AndroidManifest.xml: no android:networkSecurityConfig attribute present
# no network_security_config.xml resource found in the APK at all
# falls back to Android platform defaults: system CAs, cleartext
# permitted on Android < 9, no pinning of any kind
```

Impact: A person using running.COACH on any untrusted network, a gym, a race venue, a public trail with open WiFi, has their real-time heart-rate and exercise data exposed to interception or manipulation with no technical barrier the app itself provides.

Fix: Add a network_security_config.xml enforcing certificate pinning on all API endpoints and disabling cleartext traffic entirely, regardless of Android version. No confirmation that this has occurred was ever received.

H2: Huawei HMS Activity Recognition, an Undisclosed PRC-Subject Data Recipient

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

com.huawei.hms.permission.ACTIVITY_RECOGNITION is declared, and Huawei HMS SDK classes are present in the binary. Huawei's activity-recognition component tracks movement patterns, running, walking, stationary, linked to a Huawei advertising identifier, and transmits this to Huawei, a PRC-incorporated entity subject to China's National Security Law Art. 7, which compels cooperation with national intelligence operations without judicial review or subject notification. No adequacy decision for China exists under GDPR Art. 44, and Huawei is not named as a data recipient in running.COACH's privacy policy, which states no data is shared with independent third parties.

```
AndroidManifest.xml
com.huawei.hms.permission.ACTIVITY_RECOGNITION
com.huawei.android.launcher.permission.READ_SETTINGS
com.huawei.android.launcher.permission.WRITE_SETTINGS
Huawei HMS smali files: 7
```

Impact: When a user runs, how often, and at what times of day, behavioral data derived from activity recognition, flows to a PRC-subject company with no disclosed legal basis and no adequacy decision covering the transfer.

Fix: Name Huawei HMS individually as a data recipient with a stated Art. 44 transfer mechanism, or remove the dependency if it is not load-bearing for core functionality. No confirmation that this has occurred was ever received.

H3: Sentry, 1,136 Classes With Registered ContentProviders, Plus Background Health-Data Reads, Neither Disclosed

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

Sentry (1,136 smali classes) ships with registered ContentProviders (SentryInitProvider, SentryPerformanceProvider), the same developer organization ('runna') also used by a sibling application. Separately, android.permission.health.READ_HEALTH_DATA_IN_BACKGROUND means the app reads Health Connect data, including heart rate and exercise records, even when it is not in the foreground. Neither Sentry's presence nor the scope of background health-data access is named in running.COACH's privacy policy.

```
io.sentry.android.core.SentryInitProvider (ContentProvider, auto-init=false)
io.sentry.android.core.SentryPerformanceProvider (initOrder=200)
total Sentry smali classes: 1,136

android.permission.health.READ_HEALTH_DATA_IN_BACKGROUND
```

Impact: A performance-monitoring and error-tracking infrastructure provider, undisclosed, receives session instrumentation data, and Health Connect data is accessed even when the app is closed, both outside the scope of the app's own stated data-sharing policy.

Fix: Name Sentry individually as a data recipient with a stated legal basis, and document the specific purpose and scope of background Health Connect access. No confirmation that this has occurred was ever received.

Impact Analysis

H1 stands apart from the other findings in kind, not just severity: C1, H2, and H3 describe undisclosed data recipients contradicting the app's own privacy policy, real transparency failures, but not independently exploitable. H1 describes the complete absence of a network security configuration on an app whose core product is real-time health data, a finding that reaches HIGH on CVSS alone and is escalated here specifically because the app's realistic use context, gyms, races, public running routes, puts users on exactly the kind of untrusted networks this finding leaves them exposed on.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR and Swiss nDSG provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
nDSG Art. 19, GDPR Art. 13(1)(e)	C1	Health and training data backed up to an undisclosed third party (Google), contradicting the app's own no-sharing policy.
GDPR Art. 32, nDSG Art. 8	C2	Hardcoded Firebase credential, enabling potential project-level tampering.
GDPR Art. 32(1)(a)	H1	No network security configuration; real-time health data unprotected against interception.
GDPR Art. 44, nDSG Art. 16	H2	Undisclosed PRC-subject data recipient, no adequacy decision for the transfer.
GDPR Art. 13(1)(e)	H3	Undisclosed performance-monitoring recipient; undocumented scope of background health-data access.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, H1 is escalated from HIGH/7.1 to CRITICAL because the app's realistic use context puts its unprotected real-time health data directly at risk on untrusted networks, a circumstance CVSS's technical vector does not capture; C2, H2, and H3 correct down to MEDIUM and C1 corrects down to LOW to match their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: running.COACH-2026-R1.