



Coordinated Security & Privacy Disclosure, Final Report

adidas Running (Runtastic) for Android (com.runtastic.android)

The first health platform in this research series confirmed running behavioral ad auctions on heart-rate and blood-glucose data, a bug-bounty redirect, then eleven weeks of silence

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, ONE REDIRECT, ELEVEN WEEKS OF SILENCE SINCE

Target	adidas AG, Herzogenaurach, Germany
Product audited	adidas Running (Runtastic) for Android, com.runtastic.android, v14.8.0
Disclosure reference	REF ADIDASRUNNING-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Firebase keys / C2 zero certificate pinning, CVSS v4.0 9.3)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1	Executive Summary	3
2	Subject & Operator Analysis	4
3	Positive Observations	4
4	Findings	4
4.1	C1: Three hardcoded Firebase production API keys, the highest credential exposure in this research series	4
4.2	C2: Zero certificate pinning on a platform processing heart rate, GPS routes, and blood glucose data	5
4.3	C3: Behavioral ad auctions running on heart-rate and blood-glucose data . . .	5
4.4	H1: New Relic session replay: screen recording on a health platform	6
4.5	H2: Facebook SDK links exercise behavior to Meta profile without account connection	6
4.6	H3: SAP Emarsys: exercise behavior repurposed for marketing	7
4.7	H4: Confirmed blood glucose data access, no stated purpose in a running app	7
4.8	H5: RECORD_AUDIO: undisclosed microphone scope during outdoor workouts	8
5	adidas's Response, Recorded in Full	8
6	Data Protection, Article by Article	9
7	Disclosure Timeline & Outcome	10
8	Residual Risk & Recommendations	10

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production adidas Running Android application and identified eight findings, three CRITICAL, five HIGH. The most significant: adidas Running declares ACCESS_AD SERVICES_CUSTOM_AUDIENCE, the Android Protected Audience API for on-device behavioral ad-auction processing, and is the first health-tracking platform confirmed to use this permission in RFI-IRFOS's 17-app research series, deriving behavioral interest groups from real-time heart rate, GPS exercise routes, calorie expenditure, exercise intensity zones, and workout frequency, all Art. 9 special-category health data.

Separately, three hardcoded Firebase production keys, described by RFI-IRFOS as the highest single credential exposure in its research series, remain embedded with no rotation possible short of a new release, and the app runs zero certificate pinning on a platform that also processes heart rate, exercise routes, and, per a confirmed runtime error string, blood glucose data via Android Health Connect. Five further findings raise separate concerns: New Relic session replay recording screens showing biometric and blood-glucose data; the Facebook SDK linking exercise patterns to a user's Meta profile via device identifier without an account connection; SAP Emarsys repurposing workout data for marketing; confirmed blood-glucose data access with no stated purpose in a running app; and undisclosed microphone scope during outdoor voice-coaching sessions.

Eight written notices were sent over 91 days. adidas Information Security replied once, twelve days after R1, redirecting to its bug bounty program. RFI-IRFOS declined the redirect the same day. No reply of any kind, from that team or any other adidas address, followed across six further written notices and eleven weeks through the close of the embargo.

Scope: Static analysis of the publicly downloaded production adidas Running Android APK, on an authorized test device, only. No adidas account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to dataprotection@adidas.com and adidasPrivacy@adidas.com, bcc CERT.at and Bavaria's BayLDA. adidas Information Security replied on 2 July, redirecting to its bug bounty program. RFI-IRFOS declined the redirect the same day and escalated. No further reply of any kind was received across six subsequent written notices and eleven further weeks.

ID	Severity	Title
C1	CRITICAL	Three hardcoded Firebase production API keys, the highest credential exposure in this research series
C2	CRITICAL	Zero certificate pinning on a platform processing heart rate, GPS routes, and blood glucose data
C3	CRITICAL	Behavioral ad auctions running on heart-rate and blood-glucose data

ID	Severity	Title
H1	HIGH	New Relic session replay: screen recording on a health platform
H2	HIGH	Facebook SDK links exercise behavior to Meta profile without account connection
H3	HIGH	SAP Emarsys: exercise behavior repurposed for marketing
H4	HIGH	Confirmed blood glucose data access, no stated purpose in a running app
H5	HIGH	RECORD_AUDIO: undisclosed microphone scope during outdoor workouts

Subject & Operator Analysis

adidas AG (Herzogenaurach, Germany) operates adidas Running (formerly Runtastic) for a global fitness-tracking user base, with Bavaria's BayLDA as lead supervisory authority.

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: Three hardcoded Firebase production API keys, the highest credential exposure in this research series

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

Three distinct Firebase API keys are hardcoded in the production APK, described by RFI-IRFOS as the highest credential exposure across its 17-app research series to date.

```
AIzaSyA_VqJHowZubggLRJb_lheVmgNgr1B7bXA
AIzaSyCw83iPxH12QGXIIncUP9Be2Jv0ln24HYP8
AIzaSyD4b_38AEK7oP0PfCM6zwMt3j-hhq1Qn6Y
Database: https://runtastic-com-api-project-190569399906.firebaseio.com
```

No response was received naming this finding. The linked database is deactivated, but all three keys remain permanently embedded in every installed version of the app and cannot be rotated without a new APK release.

Impact: Three publicly extractable production credentials, embedded with no rotation path short of a new release, enable probing and potential further backend access.

Fix: Ship a new release rotating all three credentials, and restrict replacements to the production certificate fingerprint.

C2: Zero certificate pinning on a platform processing heart rate, GPS routes, and blood glucose data

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

No network security configuration was found. A platform processing health.READ_HEART_RATE, health.READ_EXERCISE_ROUTES, health.READ_TOTAL_CALORIES_BURNED, biometric authentication, and blood glucose data operates with zero TLS certificate pinning.

No response was received naming this finding. All connections are susceptible to interception on any network where a trusted-but-hostile certificate authority is present.

Impact: Health, biometric, and exercise-route traffic has no application-level protection against a compromised or hostile certificate authority.

Fix: Implement certificate pinning for all production API endpoints handling health and location data.

C3: Behavioral ad auctions running on heart-rate and blood-glucose data

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

adidas Running declares all four Android Ad Services permissions, including ACCESS_AD_SERVICES_CUSTOM_AUDIENCE, the Android Protected Audience API for on-device behavioral ad-auction processing. Only one other app in RFI-IRFOS's entire 17-app research series, Facebook, previously held this permission; adidas Running is the first health platform confirmed to use it.

Behavioral interest groups derived from:

- real-time heart rate per session
- GPS exercise routes (where, how often, what time of day)
- calorie expenditure
- exercise intensity zones (HeartRateFeatureAttributes\$Zone)
- workout frequency patterns

No response was received naming this finding, including whether ACCESS_AD_SERVICES_CUSTOM_AUDIENCE is disclosed as Art. 22 automated decision-making with an Art. 9(2)(a) explicit consent basis, restated as a yes/no question on 4 September. All of the listed signal categories constitute Art. 9 special-category health data.

Impact: On-device behavioral ad auctions run on special-category health data with no confirmed explicit consent basis distinct from a bundled terms-of-service acceptance.

Fix: Disclose ACCESS_AD_SERVICES_CUSTOM_AUDIENCE as Art. 22 automated decision-making, obtain explicit Art. 9(2)(a) consent specific to this processing, or disable behavioral ad auctions on health-signal categories.

H1: New Relic session replay: screen recording on a health platform

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

New Relic, the largest third-party SDK in the app at 859 classes, includes session replay recording every tap, scroll, and screen interaction, including workout setup, heart-rate target configuration, health-goal entries, and any screen displaying biometric, blood-glucose, or body-weight data.

No response was received naming this finding, including whether New Relic session replay is disclosed as a data recipient under Art. 13(1)(e), restated as a yes/no question on 4 September.

Impact: Full-session screen recordings, including biometric and blood-glucose data displays, are transmitted to a US processor.

Fix: Disable session replay on screens displaying health, biometric, or blood-glucose data, and name New Relic as a data recipient under Art. 13(1)(e).

H2: Facebook SDK links exercise behavior to Meta profile without account connection

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

132 Facebook SDK classes transmit device identifiers and behavioral events to Meta's advertising infrastructure, enabling exercise-pattern linkage to a user's Facebook/Instagram profile via device identifier, including for users who never connected their adidas Running account to Facebook.

No response was received naming this finding.

Impact: Exercise behavioral patterns are linked to a user's Meta profile via device identifier without an explicit account-connection action.

Fix: Disable device-identifier-based Meta linkage for users who have not explicitly connected their Facebook account.

H3: SAP Emarsys: exercise behavior repurposed for marketing

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

595 SAP Emarsys classes with a Predict module transmit workout behavioral data, exercise frequency, training plan progress, and app engagement, to SAP's marketing cloud for commercial recommendation targeting.

No response was received naming this finding. Health data collected for fitness tracking is repurposed for marketing optimization with no separate disclosed purpose.

Impact: Fitness data is repurposed for marketing optimization beyond its stated fitness-tracking purpose.

Fix: Disclose SAP Emarsys's marketing use of workout data separately from the core fitness-tracking purpose, per Art. 5(1)(b).

H4: Confirmed blood glucose data access, no stated purpose in a running app

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

The production APK contains the runtime error string "null cannot be cast to non-null type androidx.health.connect.client.records.BloodGlucoseRecord", confirming code paths that access blood glucose data via Android Health Connect.

No response was received naming this finding, including whether this access path has been reviewed and, if not required, removed, restated as a yes/no question on 4 September. Blood glucose is an unambiguous Art. 9 clinical diabetes indicator with no stated purpose in a running application.

Impact: A confirmed code path accesses clinical blood-glucose data with no disclosed purpose relevant to a fitness-tracking application.

Fix: Remove the BloodGlucoseRecord access path unless a specific, disclosed purpose requires it.

H5: RECORD_AUDIO: undisclosed microphone scope during outdoor workouts

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

RECORD_AUDIO serves the voice-coaching feature (VoiceFeedbackDownloadManager).

No response was received naming this finding. The scope of audio capture during outdoor workouts, whether it is processed locally or transmitted, and whether third-party SDKs including New Relic session replay have access to audio data during sessions, is undisclosed.

Impact: The scope and processing location of microphone data captured during outdoor workouts is undisclosed, including potential third-party SDK access.

Fix: Disclose the specific scope of RECORD_AUDIO usage and confirm whether any third-party SDK has access to audio captured during voice-coaching sessions.

adidas's Response, Recorded in Full

On 2 July 2026, adidas's Information Security team replied, in full: "Thanks for contacting the adidas Information Security team and reporting the below issue. We appreciate your efforts. The issue will be validated by our team before confirming the next steps. We will get back to you with an update shortly. We are also pleased to let you know about our private bug bounty program. To get started, please share the details of any vulnerabilities... via email... Once we receive your report, our team will conduct an initial validation check. If the vulnerability is new to us, we would be thrilled to invite you to join the adidas bug bounty program."

RFI-IRFOS declined the bug-bounty routing the same day and escalated, adding Bavaria's BayLDA and the Austrian DSB to CC. No further reply, from Information Security or any other adidas address, was received across six subsequent written notices, each restating that the promised validation update never arrived, through the close of the embargo.

Finding	Provision	Concern
---------	-----------	---------

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b), Art. 25(1)	Hardcoded, non-rotatable production credentials
C2	GDPR Art. 32(1)(a)	Zero certificate pinning on a health data platform
C3	GDPR Art. 9(2)(a), Art. 22, Art. 13(2)(f), Art. 6(1), Art. 5(1)(b)	Behavioral ad auctions on Art. 9 health data
H1	GDPR Art. 5(1)(c), Art. 9, Art. 32, Art. 13	Screen recording of biometric/blood-glucose displays
H2	GDPR Art. 5(1)(c)	Device-identifier profile linkage without account connection
H3	GDPR Art. 5(1)(b)	Health data repurposed for marketing
H4	GDPR Art. 5(1)(c), Art. 9	Undisclosed clinical blood-glucose data access
H5	GDPR Art. 5(1)(c)	Undisclosed microphone scope

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to dataprotection@adidas.com and adidasPrivacy@adidas.com, bcc CERT.at/BayLDA, 8 findings
2026-06-28	Follow-up #1, deadline set for 2 July
2026-07-02	adidas Information Security replies, redirects to bug bounty program; RFI-IRFOS declines same day and escalates
2026-07-24 / 08-05 / 08-15 / 08-24	Follow-ups restate all findings and three standing questions, Art. 33(4) 72-hour clock argument invoked
2026-08-31 / 09-04	Final follow-ups; weekly SHA-256 re-pull instituted, deadline set and passed unanswered
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Eight written notices across 91 days produced one reply, a bug-bounty redirect twelve days after R1. No further reply of any kind followed across six subsequent written notices and eleven further weeks. All eight findings, including behavioral ad auctions run on heart-rate and blood-glucose data, stand exactly as originally reported.

Residual Risk & Recommendations

- Disable ACCESS_AD SERVICES_CUSTOM_AUDIENCE on health-signal categories or obtain explicit Art. 9(2)(a) consent specific to behavioral ad auctions; this is the single highest-priority item given confirmed processing of Art. 9 health data for advertising purposes.
- Ship a release rotating all three Firebase credentials and implement certificate pinning.
- Remove the confirmed BloodGlucoseRecord access path unless a specific purpose requires it.
- Disable New Relic session replay on health and biometric data screens.
- Provide the validation update adidas Information Security promised on 2 July 2026 and never delivered.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. Research

