Coordinated Security & Privacy Disclosure, Final Report

Meine AOK for Android (de.aoksystems.amg)

Twelve written notices, ninety days, one reply asking only to verify authenticity, zero of three questions ever answered

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – THREE FINDINGS UNADDRESSED ON A STATUTORY HEALTH INSURER'S APP SERVING 26 MILLION MEMBERS

Target	AOK Systems GmbH, Kortrijker Str. 1, 53177 Bonn, Germany
Product audited	Meine AOK for Android, de.aoksystems.amg – serving AOK's approximately 26 million statutory health-insurance members
Disclosure reference	REF AOK-2026-R1-001
R1 sent	2026-06-22 (bounced), corrected delivery 2026-06-30
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C1 an unrestricted Firebase/Google API key on a health insurer's app serving 26 million members, CVSS v4.0 8.8, unaddressed)

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 performed static analysis of the production Meine AOK Android application, the mobile app for Germany's largest statutory health insurance system, serving approximately 26 million members, and identified one CRITICAL and two HIGH findings: a hardcoded Firebase/Google API key with no confirmed application restriction, capable of quota or billing exhaustion, a denial-of-service risk to real insured members if the key is abused, and potential data exposure if Firebase security rules are misconfigured, an Adobe Marketing Mobile SDK profiling in-app navigation and usage behavior within a statutory health-insurer app and transmitting it to Adobe Inc.'s US infrastructure, with Adobe not named as a data recipient in AOK's published privacy notice, and undocumented legal basis and processor-chain disclosure for ACTIVITY_RECOGNITION, ACCESS_FINE_LOCATION, and CAMERA permissions used by the app's wellness and bonus program, an Art. 9-relevant combination for a health-insurance context.

Across twelve written notices over ninety days, spanning an initial bounced attempt and two subsequent delivered threads, the only reply RFI-IRFOS ever received, on 7 July from AOK Systems' designated Datenschutzbeauftragter, Winfried Jonas, asked only for confirmation that the disclosure genuinely originated from the institute, since it had arrived from a Gmail address rather than an institutional domain. RFI-IRFOS confirmed the same day and restated all findings and three standing questions. No further reply of any kind ever addressed the Firebase key's restriction status, the Art. 46 transfer mechanism for the Adobe US transfer, or whether an Art. 35 DPIA exists for the app's Art. 9-relevant health-data processing.

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

Disposition

The original R1 sent 22 June 2026 to datenschutz@aok-systems.de bounced immediately (address does not exist); corrected delivery followed 30 June to Winfried Jonas, AOK Systems' designated Datenschutzbeauftragter, identified via the company's own Impressum. Across twelve written notices over ninety days, the only reply received, on 7 July, asked RFI-IRFOS to confirm the disclosure genuinely originated from the institute, since it arrived from a Gmail address; RFI-IRFOS confirmed the same day. No further reply of any kind addressed any of the three substantive GDPR questions.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase/Google API key with no confirmed application restriction
H1	HIGH	Adobe Marketing Mobile SDK profiling routed to the US, undisclosed
H2	HIGH	Undocumented legal basis for wellness-program device permissions

Subject & Operator Analysis

AOK Systems GmbH, based in Bonn, Germany (Handelsregister Bonn HRB 17142), develops IT systems for the AOK statutory health insurance federation, whose Meine AOK app serves approximately 26 million insured members.

Findings

C1: Hardcoded Firebase/Google API key with no confirmed application restriction

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:H/SC:N/SI:N/SA:N, 8.8

res/values/strings.xml contains google_api_key AIzaSyCmnFIJknBUE_C0aY5WEWmKxbCR5n6HDKs, google_app_id 1:750775627705:android:72537b0cbd5e14434c5068, project meine-aok. No confirmation that the key is restricted to the app's package name and signing fingerprint was ever received.

An unrestricted key permits quota or billing exhaustion, denial of service to real insured members once the quota is hit, and, if Firebase security rules are misconfigured, potential data exposure. The burden of demonstrating the key is restricted and the rules are locked lies with AOK. No reply of any kind confirmed either.

Impact: Real insured members could be denied service if the exposed key's quota is exhausted by an unrelated party, and data exposure risk cannot be ruled out without confirmation of Firebase security rule configuration.

Fix: Restrict the key to the correct package name and SHA-256 signing fingerprint, confirm Firebase security rules are deny-by-default, and publish that confirmation.

H1: Adobe Marketing Mobile SDK profiling routed to the US, undisclosed

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 binary embeds the Adobe Marketing Mobile SDK (com/adobe/marketing/mobile/analytics/internal/), profiling in-app navigation and usage behavior inside a statutory health-insurer app and transmitting it to Adobe Inc.'s US infrastructure. Adobe is not named as a data recipient in AOK's published Datenschutzerklaerung.

No reply of any kind confirmed the Art. 6 legal basis or the Art. 46 transfer mechanism (SCCs plus a transfer impact assessment) for this transfer.

Impact: In-app navigation behavior on a health-insurer app, an Art. 9 context, is transmitted to a named US processor with no matching Art. 13(1)(e)/(f) disclosure or confirmed transfer mechanism.

Fix: Name Adobe explicitly as a data recipient in the privacy notice, and document the Art. 46 transfer mechanism covering this specific data flow.

H2: Undocumented legal basis for wellness-program device permissions

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

ACTIVITY_RECOGNITION, ACCESS_FINE_LOCATION, and CAMERA permissions are used for the app's wellness and bonus program, an Art. 9-relevant combination given the health-insurance context.

This finding was raised in RFI-IRFOS's original 22 June notice, which bounced due to an incorrect recipient address, and was not restated in the corrected delivery that actually reached AOK Systems on 30 June or in any subsequent notice. AOK Systems has therefore never actually been informed of this specific finding through a delivered message; it is reported here for completeness and technical accuracy, distinct from C1 and H1, which were confirmed delivered and never substantively addressed.

Impact: Activity, precise location, and camera data used for a wellness program may be processed without a documented Art. 9(2) legal basis or disclosed processor chain.

Fix: Document and publish the Art. 9(2) legal basis and processor chain for the wellness-program permissions.

One Reply, Asking Only Whether the Sender Was Real

Across twelve written notices and ninety days, the only reply this case ever produced came on 7 July from AOK Systems' designated Datenschutzbeauftragter, Winfried Jonas, and its full content was a request to confirm the disclosure genuinely originated from RFI-IRFOS, since it had arrived from a Gmail address rather than an institutional domain. RFI-IRFOS confirmed the institute's legitimacy and registration details the same day and restated all findings and three standing questions. No further reply of any kind, from Jonas or anyone else at AOK Systems, ever addressed those questions across five further notices through 16 September.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Unrestricted API key risking quota exhaustion and possible data exposure
H1	GDPR Art. 13(1)(e)(f), Art. 44, Art. 46	Undisclosed US transfer of health-app usage behavior
H2	GDPR Art. 9	Undocumented legal basis for wellness-program device permissions

Disclosure Timeline & Outcome

Date	Event
2026-06-22	Original R1 sent to datenschutz@aok-systems.de, bounces immediately
2026-06-30	Corrected delivery to Winfried Jonas (DSB), identified via AOK's Impressum; restates C1 and H1; LDI NRW bcc'd from this point
2026-07-07	Jonas replies asking only for authenticity confirmation; RFI-IRFOS confirms the same day and restates findings
2026-08-09	Follow-up cc's the Austrian DSB and the EDPS
2026-09-04	Follow-up confirms the authenticity question resolved, restates all findings, sets a deadline of 11 September, discloses weekly SHA-256 re-hashing during the embargo
2026-09-16	Final pre-disclosure notice, flagged as likely the last message before publication
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Confirm and publish that the exposed Firebase key is restricted by package name and signing fingerprint, and that security rules are deny-by-default.
- Name Adobe explicitly as a data recipient and document the Art. 46 transfer mechanism for US-bound usage data.
- Document the Art. 9(2) legal basis and processor chain for wellness-program device permissions.
- Establish a functioning datenschutz@ mailbox, given the original notice bounced due to a nonexistent address.

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 Coordinated disclosure per ISO/IEC 29147. GDPR Art. 9, 13, 32, 35, 44, 46. REF AOK-2026-R1-001.