Coordinated Security & Privacy Disclosure, Final Report

Mein A1 for Android (at.mobilkom.android.meina1)

Eight written notices, ninety days, genuine ongoing internal review acknowledged but never concluded

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – FOUR FINDINGS STILL OPEN, INTERNAL REVIEW ACKNOWLEDGED BUT NEVER CONCLUDED

Target	A1 Telekom Austria AG
Product audited	Mein A1 for Android, at.mobilkom.android.meina1
Disclosure reference	REF MEINA1-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (H1 a competitor's carrier-measurement SDK starting on boot with background GPS regardless of consent state, CVSS v4.0 8.7, unresolved)

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 Findings 4
3.1 C1: Firebase API key hardcoded in the Play Store binary 4
3.2 H1: A competing carrier's SDK starts on boot with background GPS regardless of consent 5
3.3 H2: allowBackup=true with incomplete exclusion rules 5
3.4 H3: Facebook SDK codeless event tracking on a carrier self-service app . . . 6

4 A Genuine Review, Never Confirmed Complete 6

5 Data Protection, Article by Article 6

6 Disclosure Timeline & Outcome 7

7 Residual Risk & Recommendations 7

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Mein A1 Android application and identified one CRITICAL and three HIGH findings: a Firebase API key hard-coded in the shipped APK, present in every published binary since first release, a Vodafone NetPerform SDK, from a competing carrier, holding BIND_CARRIER_SERVICES permission and an exported boot receiver that starts network-quality measurement with background GPS regardless of the app's own two consent flows on fresh installs, an allowBackup configuration whose exclusion rules cover only two specific preference files while account status, contract information, data-usage data, OneSignal state, Facebook SDK state, and all SQLite databases are backed up in full to the user's Google account, and a Facebook SDK integration performing codeless UI-interaction event tracking, which areas of the app users visit, time spent on billing pages, contract upgrades viewed, transmitted to Meta Platforms in the US, with the app's own privacy settings listing only a subset of that tracking scope.

Unlike most cases in this disclosure wave, A1's privacy and legal contact, Gert Paulhart, engaged genuinely and repeatedly, if slowly: he confirmed on 2 July that A1 could not locate the original 21 June message but had received the 28/30 June resends, stated an internal review had already been initiated, and on 3 August apologized for the delay and asked for continued patience while that review remained ongoing. No dismissal, denial, or refusal was ever issued. However, as of the 19 September embargo date, none of RFI-IRFOS's three standing questions, the Art. 6(1) legal basis for the NetPerform SDK's boot-triggered background location collection, whether the Austrian DSB was notified under Art. 33 of the hardcoded Firebase key, and whether an Art. 35 DPIA was conducted for the Facebook SDK's US data transfer, had received a substantive answer, and the internal review Paulhart described was never confirmed complete.

Scope: Static analysis of the publicly downloaded production Mein A1 Android APK, on an authorized test device, only. No A1 account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@a1.at, bcc the Austrian Datenschutzbehoerde and CERT.at. A1's privacy and legal contact, Gert Paulhart, engaged genuinely across the case: he could not locate the original 21 June message internally, confirmed receipt of the 28/30 June resends, stated an internal review had been initiated, and on 3 August asked for continued patience while that review remained ongoing. As of the embargo date, none of the three standing technical questions had received a substantive answer, and no publication/closure correspondence had yet been exchanged specific to this app.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the Play Store binary
H1	HIGH	A competing carrier's SDK starts on boot with background GPS regardless of consent

ID	Severity	Title
H2	HIGH	allowBackup=true with incomplete exclusion rules
H3	HIGH	Facebook SDK codeless event tracking on a carrier self-service app

Subject & Operator Analysis

A1 Telekom Austria AG is Austria's largest telecommunications operator. Related sibling apps under the same controller, yesss! and Red Bull MOBILE eSIM, surfaced overlapping findings during this correspondence and are covered separately.

Findings

C1: Firebase API key hardcoded in the Play Store binary

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

google_api_key / google_crash_reporting_api_key AIzaSyBYAFbLEHBtxNobOacHrvDskpevjb92A2I, project mein-a1-prod, firebase_database_url https://mein-a1-prod.firebaseio.com, App ID 1:834968792196:android:c062028d540fbe96, present in every published binary since first release.

Whether the Austrian DSB was notified under Art. 33 of this exposure was one of three standing questions never substantively answered.

Impact: A production Firebase project's attack surface cannot be independently ruled safe from outside the console once its key ships in every installed client, and here has done so since the app's first release.

Fix: Rotate the exposed key, confirm deny-by-default security rules, and enforce App Check for this project.

H1: A competing carrier's SDK starts on boot with background GPS regardless of consent

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 Vodafone NetPerform SDK v11.0.0 (100 smali classes) holds BIND_CARRIER_SERVICES permission, and its RebootIntentReceiver, an exported component, triggers on BOOT_COMPLETED and starts the measurement service before the user opens the app, using ACCESS_BACKGROUND_LOCATION and ACCESS_FINE_LOCATION for GPS-tagged network-quality measurements. Two consent flows exist for anonymous and personalized data, but the boot receiver starts regardless of consent state on fresh installs.

The legal basis for transmitting carrier-quality data to Vodafone, a direct competitor to A1, before any consent decision is made, was one of three standing questions never substantively answered.

Impact: Background location-tagged network measurement data may reach a competing carrier's infrastructure before a user has made any consent decision.

Fix: Gate the boot-triggered NetPerform service behind the existing consent flows so it never starts before a consent decision is recorded.

H2: allowBackup=true with incomplete exclusion rules

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

data_extraction_rules.xml excludes only SecurePreferences.xml and credentials.xml from cloud backup; no database exclusions are configured. Cached account status, contract information, data-usage data, OneSignal state, Facebook SDK state, and all SQLite databases are backed up to the user's Google account. The same gap exists in the legacy full_backup_content.xml.

No reply of any kind confirmed whether this exclusion gap has been remediated.

Impact: Contract and usage data beyond the two explicitly excluded files is backed up to a user's personal cloud storage with no comprehensive exclusion policy.

Fix: Extend data_extraction_rules.xml and full_backup_content.xml to exclude all account, contract, usage, and third-party SDK state, not only the two currently listed files.

H3: Facebook SDK codeless event tracking on a carrier self-service 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

125 smali classes implement AppEventsLogger and codeless event tracking (EventBinding, PathComponent, ModelManager$Task), sending UI-interaction behavioral events, which areas of the app users visit, time spent on billing pages, contract upgrades viewed, to Meta Platforms Inc. (Menlo Park, USA). The app's own privacy settings UI lists fb_analytics/fb_remote_conf, but the codeless tracking's actual scope may exceed what is disclosed there.

Whether an Art. 35 DPIA was conducted for this US data transfer was one of three standing questions never substantively answered.

Impact: Detailed billing and contract-interaction behavior on a carrier self-service app may be transmitted to a US recipient beyond what the app's own privacy disclosure describes.

Fix: Audit the codeless tracking configuration against the disclosed scope and correct any mismatch, and confirm an Art. 35 DPIA covers this transfer.

A Genuine Review, Never Confirmed Complete

A1's privacy and legal contact, Gert Paulhart, is one of the few correspondents in this disclosure wave to engage repeatedly and in good faith: confirming what had and had not reached his team, stating an internal review had begun, and explicitly asking for patience while it continued. No dismissal, denial, or refusal was ever issued. But across eight notices and ninety days, that review was never confirmed complete, none of the three standing technical questions received a substantive answer, and no publication or closure correspondence specific to Mein A1 exists in the record as of the embargo date.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32, Art. 33	Hardcoded Firebase key, notification status unconfirmed
H1	GDPR Art. 6(1)	Boot-triggered background location data reaching a competing carrier
H2	GDPR Art. 32	Incomplete cloud-backup exclusion for account and contract data
H3	GDPR Art. 13(1)(e), Art. 35, Art. 46	Codeless behavioral tracking possibly exceeding disclosed scope

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@a1.at, bcc Austrian DSB/CERT.at; 1 CRITICAL + 3 HIGH findings; a EUR 75,000 remediation figure was referenced under the R1 policy then in force – historical record only, not a currently open offer
2026-07-01	Paulhart queries the emails' authenticity; RFI-IRFOS confirms registry details the same day
2026-07-02	Paulhart confirms receipt of the 28/30 June resends, states an internal review has begun
2026-08-03	Paulhart apologizes for the delay, asks for continued patience while the review remains ongoing
2026-09-03	RFI-IRFOS sends an update referencing the related Red Bull MOBILE eSIM case within the same controller
2026-09-19	Embargo, as stated in the original R1, is reached; no publication/closure correspondence specific to Mein A1 exists in the record, and this report publishes

Residual Risk & Recommendations

- Conclude and communicate the outcome of the internal review referenced since 2 July.
- Gate the NetPerform boot-triggered service behind the app's existing consent flows.
- Extend cloud-backup exclusion rules to cover account, contract, usage, and third-party SDK state.
- Rotate the exposed Firebase key and confirm Art. 33 notification status.
- Audit Facebook SDK codeless tracking scope against the disclosed privacy-settings description.

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. 6, 13, 32, 33, 35, 46. REF MEINA1-2026-R1.