Coordinated Privacy Disclosure, Final Report

marktguru Android (com.marktguru.android)

marktguru GmbH / Bonial International GmbH, a ProSiebenSat.1 Media SE group company, Berlin, Germany

DISPUTED, NO TECHNICAL REBUTTAL PROVIDED · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, TWO DAYS AFTER THE EMBARGO

Target	marktguru, a supermarket leaflet and deals Android app
Package	com.marktguru.android
Operator	marktguru GmbH / Bonial International GmbH, Axel-Springer-Str. 65, 10888 Berlin; legal matters handled by ProSiebenSat.1 Media SE's central legal department
Initial Disclosure	2026-06-25
Original Embargo	2026-09-23 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, two days after the embargo, an internal publishing gap, not a change in terms
Regulators	Berlin data protection authority BlnBDI (lead SA), Austrian DSB, CERT.at
Total Outbound Messages	9, across 92 days: five to datenschutz@marktguru.de between 25 June and 3 July 2026, four further to ProSiebenSat.1 Media SE's legal department between 7 July and 3 September 2026, restating the three original open questions each time.
Inbound Replies	1, a formal cease-and-desist letter from ProSiebenSat.1 Media SE's legal department on 7 July 2026, asserting that a technical review found the allegations unfounded and demanding retraction, without identifying any specific finding as factually incorrect. No technical rebuttal of any individual finding was ever received.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to marktguru GmbH that its supermarket leaflet and deals Android app requests ACCESS_BACKGROUND_LOCATION, Android's highest-privilege location permission, for store-proximity notifications, and routes that geofencing through Huawei HMS Location Services. Huawei Technologies Co., Ltd. is a PRC-incorporated company subject to China's National Security Law Art. 7, an obligation to cooperate with PRC state intelligence on demand, without a court order or user notification. EU users' real-time background location, plausibly revealing home and workplace patterns, transits this infrastructure with no EU adequacy decision covering the transfer.

On 7 July 2026, ProSiebenSat.1 Media SE's central legal department, which handles marktguru's legal affairs, sent a formal cease-and-desist letter. It stated that the allegations had been technically reviewed and found unfounded, demanded that RFI-IRFOS retract all public statements about the findings by 10 July 2026, and warned of civil and criminal consequences for non-compliance. The letter did not identify a single specific finding as factually incorrect, name which technical claim was disputed, or offer any artifact-level rebuttal. RFI-IRFOS replied the same day and three more times over the following two months, restating the same three original technical questions, each unanswered.

Nine messages were sent across 92 days: five to the original contact address before the escalation to ProSiebenSat.1's legal department, and four more after it, cc'ing the Berlin data protection authority and CERT.at. One reply was received, the cease-and-desist letter itself; no technical rebuttal of any specific finding followed it. The 90-day embargo, set at first contact, elapsed on 23 September 2026. This report and the accompanying closure notice publish two 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 marktguru Android application (com.marktguru.android, version 2026.06.739, 23.9 MB, including the German-market split APK), as pulled via ADB from a physical device and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with marktguru's or Huawei's backend infrastructure was performed. Every artefact cited below is a static string or class reference extracted directly from the reviewed binary and independently reproducible from the same APK.

Disposition

Six findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. Background location access routed through Huawei HMS geofencing, a PRC-NSL-obligated infrastructure provider, reaches HIGH on the computed CVSS score alone, no editorial escalation needed. Pre-consent Firebase and ML Kit initialization, Facebook codeless event logging, and the Privacy Sandbox Custom Audience permission correct to MEDIUM, as does an Adjust SDK integration carrying a Chinese advertising identifier (OAID). A boot-time auto-start receiver corrects to OBSERVATIONAL. ProSiebenSat.1 Media SE's legal department sent a cease-and-desist letter asserting the findings were technically reviewed and found unfounded, without naming any specific finding in dispute; four further messages restating the original three questions drew no technical response of any kind.

ID	Severity	Title
C1	MEDIUM	Google ML Kit and Firebase Both Initialize Before Any Consent Screen
H1	HIGH	ACCESS_BACKGROUND_LOCATION Routed Through Huawei HMS Geofencing
H2	MEDIUM	Facebook Codeless Event Logging Captures UI Interactions Automatically
H3	MEDIUM	All Four Privacy Sandbox Permissions, Including Cross-App Custom Audience Targeting
M1	MEDIUM	Adjust SDK Carries a Chinese Advertising Identifier via Huawei/MSA
M2	OBSERVATION	Boot-Time Auto-Start

Subject & Operator Analysis

marktguru is a supermarket leaflet and deals app operated by marktguru GmbH / Bonial International GmbH, a Berlin-based company in the ProSiebenSat.1 Media SE group, whose central legal department handles marktguru's legal affairs.

Several genuine positives are worth naming. allowBackup is correctly set to false. usesCleartextTraffic is correctly set to false. A network security configuration is present. RECORD_AUDIO is justified by a confirmed voice-search feature. CAMERA is justified by a confirmed barcode-scanner product-lookup feature built on ML Kit. USE_BIOMETRIC supports a genuine secure-login feature.

A Cease-and-Desist Letter Naming No Specific Finding

This case's correspondence record includes a formal legal response, not silence. On 7 July 2026, twelve days after the original disclosure, ProSiebenSat.1 Media SE's Legal Affairs department (Data Protection & IT Law) replied on marktguru's behalf. The letter stated that the allegations had been technically reviewed and found unfounded, demanded retraction of all public statements about the findings by 10 July 2026, and referenced potential civil and criminal consequences for non-compliance. The letter did not identify which of the six findings it considered incorrect, cite a specific artefact it disputed, or offer any technical detail contradicting the static analysis. RFI-IRFOS replied the same day, and again on 27 July, 4 August, and 15 August 2026, restating the same three original technical questions on each occasion, cc'ing the Berlin data protection authority and CERT.at. None of the four follow-ups drew a further reply of any kind. Every artefact cited in this report is a static string or class reference directly extracted from the reviewed binary and independently reproducible from the same APK; RFI-IRFOS is not aware of any technical basis on which these specific artefacts could be considered inaccurate, and none was ever provided.

Findings

C1: Google ML Kit and Firebase Both Initialize Before Any Consent Screen

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.

Both MlKitInitProvider (initOrder=99) and FirebaseInitProvider (initOrder=100) are declared directBootAware="true", meaning both initialize at process creation, before any Activity and therefore before any consent screen.

```
com.google.mlkit.common.internal.MlKitInitProvider   initOrder=99, directBootAware=
    true
com.google.firebase.provider.FirebaseInitProvider   initOrder=100, directBootAware=
    true
```

Impact: Two separate SDK bootstraps begin before a user has seen a single consent notice.

Fix: Defer both providers' initialization until after an app-native consent flow has run. No specific rebuttal of this artefact was ever received.

H1: ACCESS_BACKGROUND_LOCATION Routed Through Huawei HMS Geofencing

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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

ACCESS_BACKGROUND_LOCATION, Android's highest-privilege location permission, is declared alongside ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION, used for store-proximity notifications via Huawei HMS Location Services' geofencing API. Huawei Technologies Co., Ltd. is a PRC-incorporated company subject to China's National Security Law Art. 7, an obligation to cooperate with PRC state intelligence on demand, without a court order or user notification. No EU adequacy decision exists for the PRC.

```
android.permission.ACCESS_BACKGROUND_LOCATION
com.huawei.hms.location.GeofenceRequest$Builder
com.huawei.hms.support.api.entity.location.fence.GeofenceEntity
com.huawei.permission.ACCESS_HW_KEYSTORE
```

Impact: EU users' real-time background location, capable of revealing home address, workplace, and movement patterns, transits infrastructure operated by a company legally obligated to cooperate with PRC state intelligence without notice, with no EU adequacy decision covering the transfer.

Fix: Document an Art. 44-49 transfer mechanism for the Huawei HMS geofencing pipeline or replace it with an EU-adequate provider. No specific rebuttal of this artefact was ever received.

H2: Facebook Codeless Event Logging Captures UI Interactions Automatically

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.

Facebook Codeless Event Logging attaches AutoLoggingOnClickListener to UI elements automatically, without the developer writing explicit tracking code for each interaction. Any button tap, list selection, or navigation event can be captured and transmitted based on server-side configuration not visible in the static binary. Combined with active attribution tracking, Meta can receive what deals a user browses, what supermarkets they interact with, and what offers they tap.

```
com.facebook.appevents.codeless.CodelessLoggingEventListener.
    AutoLoggingOnClickListener
com.facebook.sdk.attributionTracking  (active)
```

Impact: UI interaction data can be captured and transmitted to Meta without a developer-reviewable, code-level list of what is actually sent.

Fix: Disable codeless event logging or document the specific event set forwarded to Meta under Art. 13(1)(e). No specific rebuttal of this artefact was ever received.

H3: All Four Privacy Sandbox Permissions, Including Cross-App Custom Audience Targeting

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.

AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_TOPICS, and ACCESS_ADSERVICES_CUSTOM_AUDIENCE are all declared. Custom Audience enables marktguru to define behavioral cohorts of its own users and make those cohorts available for ad targeting inside other apps, a use exceeding what a user of a supermarket deals app would reasonably expect.

```
android.permission.ACCESS_ADSERVICES_AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_TOPICS
android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE
```

Impact: A user's supermarket-deal browsing behavior can be turned into a cross-app advertising targeting cohort without a disclosed purpose located in the app's privacy documentation.

Fix: Document an individual Art. 6(1) legal basis for Custom Audience targeting or remove the permission. No specific rebuttal of this artefact was ever received.

M1: Adjust SDK Carries a Chinese Advertising Identifier via Huawei/MSA

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.

Adjust's attribution SDK integrates OAID (a Chinese advertising identifier standard) via both Huawei HMS and the MSA SDK, with pre-install attribution enabled and a custom deep integration (AdjustInfo) confirmed in the binary.

```
com.adjust.sdk.oaid.HmsSdkClient
com.adjust.sdk.oaid.MsaSdkClient
com.adjust.preinstall.READ_PERMISSION
Lcom/marktguru/app/model/AdjustInfo
```

Impact: A Chinese-standard advertising identifier is generated and used for attribution alongside standard identifiers, widening the fingerprinting surface available to Adjust and its downstream partners.

Fix: Document the OAID integration and its purpose under Art. 13(1)(c), or disable it for EU traffic. No specific rebuttal of this artefact was ever received.

M2: Boot-Time Auto-Start

OBSERVATIONAL — not independently CVSS-scored; auto-start alone carries no direct confidentiality, integrity, or availability impact to score.

RECEIVE_BOOT_COMPLETED is declared, meaning the app starts automatically at device boot.

Impact: The app begins running at every device boot without an explicit user launch, a transparency point, not a demonstrated technical exposure on its own.

Fix: Document the purpose of boot-time auto-start, or remove it if not load-bearing for a specific, disclosed feature. No specific rebuttal of this artefact was ever received.

Data Protection, Article by Article

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

Article	Finding	Basis
Art. 7, Art. 25	C1	Pre-consent SDK initialization via direct-BootAware ContentProviders.
Art. 44-49, Art. 5(1)(c)	H1	Background location routed through a PRC-NSL-obligated infrastructure provider.
Art. 5(1)(a), Art. 13(1)(e)	H2	Undisclosed automatic UI-interaction capture forwarded to Meta.
Art. 5(1)(b), Art. 6(1)	H3	Undisclosed cross-app advertising cohort targeting.
Art. 13(1)(c)	M1	Undisclosed Chinese advertising identifier integration.

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 reaches HIGH on its computed CVSS v4.0 score alone, no editorial escalation applied; C1, H2, H3, and M1 correct to MEDIUM to match their own computed bands; M2 is classified OBSERVATIONAL because auto-start alone carries no direct scoreable impact. A cease-and-desist letter received 7 July 2026 characterized these findings as unfounded following an internal technical review, without identifying a specific disputed artefact; RFI-IRFOS notes this general characterization without accepting it, in the absence of any artefact-level rebuttal received to date. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: MARKTGURU-2026-R1.