Coordinated Security & Privacy Disclosure, Final Report

Drei Kundenzone for Android (com.hutchison3g.at.android.selfcare)

One blanket denial naming zero findings specifically, then eighty-five days and five automated ticket acknowledgments

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FIVE FINDINGS UNADDRESSED SINCE A SINGLE BLANKET DENIAL

Target	Hutchison Drei Austria GmbH, Vienna, Austria
Product audited	Drei Kundenzone for Android, com.hutchison3g.at.android.self care, v4.3.0
Disclosure reference	REF DREI-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (H1, zero certificate pinning on the carrier-billing portal, CVSS v4.0 7.1, unaddressed)

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: Hardcoded, never-rotated Firebase API key, ~2.5 million subscribers at platform scale 4

3.2 H1: Zero certificate pinning on the carrier-billing WebView portal 5

3.3 H2: GPS-precision speed test starts on every device boot, before consent . . 5

3.4 M1: Firebase Analytics active in parallel with the declared analytics provider . 6

3.5 M2: Attribution access left open to all SDKs with no visible advertising model . 6

4 One Denial, Zero Named Findings, Three Unanswered Questions 7

5 Data Protection, Article by Article 7

6 Disclosure Timeline & Outcome 8

7 Residual Risk & Recommendations 8

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Drei Kundenzone Android application, the customer self-service app for Austria's third-largest mobile carrier, and identified one CRITICAL, two HIGH, and two MEDIUM findings: a hardcoded Firebase API key whose auto-generated, never-renamed project identifier is itself forensic evidence it has never been rotated since integration; a complete absence of certificate pinning on the WebView portal handling contracts, invoices, and payment; a GPS-precision speed-test service that starts automatically on every device boot, before any user interaction or consent, using fine rather than coarse location; a Firebase Analytics SDK running in parallel with the declared analytics provider, Piwik Pro, raising an undisclosed-processor question; and an attribution configuration left open to all SDKs despite no visible advertising business model.

Five days after R1, Drei's legal/data-protection department replied once, in full: the findings do not constitute security vulnerabilities, several rest on incorrect technical assumptions or describe intended platform behavior, and Drei does not participate in paid disclosure programs. No finding was named individually, and none has been named individually since, across three direct written requests asking Drei to identify which specific finding it disputes and why.

The Firebase key finding carries particular weight given scale: Drei Kundenzone serves approximately 2.5 million subscribers, and an unrotated, publicly extractable project key of this kind can be used to probe remote configuration, send forged push notifications platform-wide, and, if Firebase security rules are not restrictive, access session data. Every subsequent inbound message after the 26 June denial, five in total across eleven weeks, was an automated ticket-system acknowledgment; no further human reply of any kind was received.

Scope: Static analysis of the publicly downloaded production Drei Kundenzone Android APK (v4.3.0), on an authorized test device, only. No Drei account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to dpo@drei.com, bcc the Austrian DSB, CERT.at, and RTR. Drei's legal/data-protection department replied once, five days later, with a blanket denial naming zero findings specifically. Across four further written follow-ups over the following eleven weeks, cc'ing the DSB, CERT.at, and RTR openly, Drei never named a single disputed finding, never answered any of RFI-IRFOS's three direct questions, and every subsequent inbound message was an automated ticket-system acknowledgment.

ID	Severity	Title
C1	CRITICAL	Hardcoded, never-rotated Firebase API key, ~2.5 million subscribers at platform scale
H1	HIGH	Zero certificate pinning on the carrier-billing WebView portal
H2	HIGH	GPS-precision speed test starts on every device boot, before consent

ID	Severity	Title
M1	MEDIUM	Firebase Analytics active in parallel with the declared analytics provider
M2	MEDIUM	Attribution access left open to all SDKs with no visible advertising model

Subject & Operator Analysis

Hutchison Drei Austria GmbH operates as Austria's third-largest mobile carrier, under the joint jurisdiction of the Austrian Datenschutzbehörde and RTR (Rundfunk und Telekom Regulierungs-GmbH) for telecommunications-specific obligations under TKG 2021.

Findings

C1: Hardcoded, never-rotated Firebase API key, ~2.5 million subscribers at platform scale

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 AIzaSyA8uPzWIXBwHGdw9ueB-V_KDOXKj3K31Z4, Firebase project tribal-quasar-143512, an auto-generated GCP project name never renamed since creation, unlike properly-maintained projects such as those seen in comparable audits.

The untouched auto-generated project name is itself forensic evidence the credential has never been rotated since Firebase integration. With this key, an attacker could probe the Firebase database and remote configuration, send forged push notifications to Drei's roughly 2.5 million subscribers, and, if Firebase security rules are not restrictive, access user session data. Drei's 26 June reply did not name this finding specifically, and no later reply addressed when, or whether, this key has ever been rotated.

Impact: A single unrotated credential exposes push-notification forgery and configuration-probing risk across the carrier's full subscriber base.

Fix: Rotate the key immediately, restrict it to the app's package name and signing fingerprint, and confirm Firebase Security Rules are deny-by-default.

H1: Zero certificate pinning on the carrier-billing WebView portal

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

No android:networkSecurityConfig attribute and no network_security_config.xml resource exist anywhere in the app. CabWebviewManager.loadInWebView() loads the carrier billing portal, contracts, invoices, and payment flows, with no certificate pins, relying on system-CA trust alone.

A comparator carrier app audited in the same wave ships seven domain configurations with SHA-256 pins expiring in 2027; Drei ships none. Unaddressed in Drei's 26 June reply or any later message.

Impact: An actor holding a system-trusted certificate, via enterprise MDM, a compromised CA, or a network-level attack, could intercept WebView traffic carrying contract and payment data.

Fix: Implement certificate pinning on the carrier-billing WebView domains, matching or exceeding the comparator carrier's configuration.

H2: GPS-precision speed test starts on every device boot, before consent

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

A BootReceiver registered for BOOT_COMPLETED and QUICKBOOT_POWERON triggers SpeedtestForegroundService, declared with foregroundServiceType="location" and ACCESS_FINE_LOCATION, on every device restart, before the user has ever opened the app.

Network-level, coarse location would suffice for carrier signal-quality geo-tagging; GPS-precision capture is data-minimization-excessive for this stated purpose. Unaddressed in any Drei reply.

Impact: Precise location data is captured at every device restart, before any consent interaction has occurred.

Fix: Gate the speedtest service behind explicit in-app consent, and use coarse rather than fine location for signal-quality benchmarking.

M1: Firebase Analytics active in parallel with the declared analytics provider

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

34 Firebase Analytics smali classes run alongside 11 Piwik Pro (Warsaw, EU) smali classes. Piwik Pro is a genuinely privacy-conscious choice relative to standard Google Analytics, but if Drei's privacy statement names only Piwik Pro, Firebase/Google as a US processor is undisclosed.

Unaddressed in any Drei reply, including whether the privacy policy has since been amended to name Firebase/Google alongside Piwik Pro.

Impact: A second analytics processor operates without a matching privacy-policy disclosure.

Fix: Name Firebase/Google Analytics explicitly in the privacy policy if it remains active, or remove it if Piwik Pro is intended as the sole provider.

M2: Attribution access left open to all SDKs with no visible advertising model

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

ga_ad_services_config.xml declares <attribution allowAllToAccess="true" />, opening attribution access to all SDKs despite the app having no visible advertising business model.

Unaddressed in any Drei reply.

Impact: Attribution data is exposed more broadly than the app's apparent purpose requires.

Fix: Restrict attribution access to the specific SDKs that require it, or disable it entirely if unused.

One Denial, Zero Named Findings, Three Unanswered Questions

Drei's only substantive reply, verbatim: "Wir haben die von Ihnen dargestellten Punkte intern einer sorgfältigen technischen Prüfung unterzogen. Auf Basis dieser Bewertung sind wir zu dem Schluss gekommen, dass die angeführten Punkte in der dargestellten Form keine Sicherheitslücken darstellen. Insbesondere beruhen mehrere der genannten Aspekte entweder auf unzutreffenden technischen Annahmen oder beschreiben vorgesehenes und übliches Platt formverhalten." RFI-IRFOS asked three times, in writing, which specific finding rests on an incorrect technical assumption and why. None was ever named.

Data Protection, Article by Article

Finding	Provision	Concern
C1	DSGVO Art. 32(1); TKG 2021 §93	Unrotated production credential at 2.5 million subscriber scale
H1	DSGVO Art. 32(1)(a), Art. 25; TKG 2021 §93	No certificate pinning on billing/contract portal
H2	DSGVO Art. 6(1)(a), Art. 5(1)(c); TKG 2021 §165	Pre-consent, excessive-precision location capture at boot
M1	DSGVO Art. 13(1)(e), Art. 46	Undisclosed second analytics processor
M2	DSGVO Art. 5(1)(c), Art. 6(1)	Attribution access open to all SDKs, no matching business need

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to dpo@drei.com, bcc Austrian DSB/CERT.at/RTR, 1 CRITICAL + 2 HIGH + 2 MEDIUM findings
2026-06-26	Drei's only substantive reply: blanket denial naming zero findings; same-day rebuttal restates each finding with source lines
2026-07-27	Follow-up, 31 days unanswered, restates the three direct questions
2026-08-09 / 08-18	Status checks add CERT.at and RTR to visible cc, restate an interim deadline
2026-09-04	Final follow-up, 70 days since the blanket denial, restates the Firebase key and certificate-pinning findings; automated acknowledgment is the last inbound message
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Name the specific finding Drei disputes as resting on an incorrect technical assumption, and explain the basis.
- Rotate the Firebase key named in C1, given the scale of Drei's subscriber base.
- Implement certificate pinning on the carrier-billing WebView portal.

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. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). DSGVO Art. 5, 6, 13, 25, 32, 46; TKG 2021 §§93, 165. REF DREI-2026-R1.