



Security & Privacy Disclosure, Final Report

VIG KV App for Android (com.vig.kvApp)

A health-insurance app that feeds claims, benefits, and prescription-browsing behavior into a US/Czech marketing-automation platform, ships an advertising-attribution configuration open to every other app on the device, and hardcodes a production Google Cloud API key, unresolved through 108 days and a 21-day-overdue embargo, with zero reply of any kind from either directly-addressed VIG mailbox

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 26
SEPTEMBER 2026, FOUR FINDINGS REMAIN UNADDRESSED**

Target	Vienna Insurance Group AG (ATX: VIG) — health insurance arm
Package	com.vig.kvApp
Platform Audited	Android · v5.4.2 (versionCode 1017216), static analysis of the production APK
Initial Disclosure (R1)	2026-06-26
Disclosure / Embargo Date	2026-09-26
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	4 (3 Critical, 1 High)
Correspondence	10 messages sent by RFI-IRFOS to datenschutz@vig.com and security@vig.com (two CC addresses, presse@vig.com and kundenservice@vig.com, bounced permanently from message one onward and were dropped). 0 responses of any kind, automated or human, ever received from either addressed mailbox.
Authorities BCC'd	Oesterreichische Datenschutzbehoerde (DSB), Finanzmarktaufsicht (FMA)

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	B1: Exponea/Bloomreach customer data platform embedded in a health-insurance claims app	6
4.2	B2: Privacy Sandbox advertising-attribution data opened to every app on the device	7
4.3	B3: Production Google Cloud API key hardcoded in the release binary	7
4.4	H1: Boot-triggered autostart combined with precise location access, no documented purpose	8
5	Impact Analysis	8
6	The Complete Chain: Ten Messages, Two Surviving Mailboxes, Zero Replies Of Any Kind, 108 Days	9
7	Data Protection — Article by Article	9
8	Regulatory & Legal Landscape	10
9	Indicators of Compromise	10
10	Disclosure Timeline & Outcome	11
11	Residual Risk & Recommendations	11

Executive Summary

The VIG KV App (com.vig.kvApp) is the Android health-insurance claims app of Vienna Insurance Group AG (ATX: VIG). Static analysis of the production binary (v5.4.2) found a full Exponea/Bloomreach customer data platform embedded in a health-claims app, an advertising-attribution configuration left open to every other app on the device, and a hardcoded Google Cloud API key, alongside one positive finding: VIG is the only insurer in this research series so far to enable certificate transparency enforcement in its network security configuration.

RFI-IRFOS identified 3 CRITICAL and 1 HIGH severity findings. B1 (CRITICAL): the app embeds the full Exponea SDK (now Bloomreach Engagement), a customer data platform and marketing-automation product, with its own database, network, telemetry, campaign-management, and in-app-messaging layers. On a health-insurance app, this means behavior while filing a claim, viewing a benefits statement, uploading a doctor's document, or browsing medication information feeds directly into a marketing-automation engine, hosted on AWS/US infrastructure via a Brno, Czech Republic vendor, with no Art. 9(2) legal basis identified in VIG's privacy notice. B2 (CRITICAL): the Android Privacy Sandbox Attribution configuration is set to allowAllToAccess="true", meaning any other app installed on the same device can read which advertising campaign led to the VIG KV App's install or open, an indirect signal of active private health-insurance shopping. B3 (CRITICAL): a Google Cloud Platform geo-services API key is hardcoded in plaintext in the production binary, readable by anyone, with a direct quota-exhaustion abuse path at VIG's cost. B4 (HIGH): the app auto-starts on every device boot via RECEIVE_BOOT_COMPLETED while holding ACCESS_FINE_LOCATION, with no documented purpose for continuous background location capture on a claims-and-benefits app.

RFI-IRFOS disclosed these findings on 26 June 2026 to datenschutz@vig.com and security@vig.com, CC presse@vig.com and kundenservice@vig.com, BCC the Austrian Datenschutzbehörde (DSB) and the Finanzmarktaufsicht (FMA). Both CC addresses bounced permanently on the first message and were dropped from the distribution list. Nine further messages followed over the next 78 days, all to the same two surviving addresses, restating the same three open questions each time. Across all ten messages, not one reply of any kind, human or automated, was ever received from datenschutz@vig.com or security@vig.com. The stated embargo of 26 September 2026 passed 21 days before this report's publication date, with all four findings unaddressed.

ID	Severity	Title
B1	CRITICAL	Exponea/Bloomreach customer data platform embedded in a health-insurance claims app
B2	CRITICAL	Privacy Sandbox advertising-attribution data opened to every app on the device
B3	CRITICAL	Production Google Cloud API key hardcoded in the release binary
H1	HIGH	Boot-triggered autostart combined with precise location access, no documented purpose

Subject & Operator Context

VIG KV App is the private health-insurance claims and benefits app of Vienna Insurance Group AG, listed on the Vienna Stock Exchange (ATX: VIG). Core functions are claims submission, benefits overview, document upload (including physician documents), and medication-information lookup, all categories of Art. 9 GDPR special-category health data.

The app's engineering baseline is mixed: it is the only insurer-category app in this research series so far to enable certificate transparency in its network security configuration, and it uses a modern Jetpack Compose architecture with biometric authentication available. That baseline makes the central finding more notable, not less: a well-built app can still embed a full marketing-automation customer data platform directly on top of health-insurance usage data.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 26 June 2026 to datenschutz@vig.com and security@vig.com, CC presse@vig.com and kundenservice@vig.com, BCC the Austrian Datenschutzbehörde and the Finanzmarktaufsicht, stating an embargo date of 26 September 2026. Both CC addresses, presse@vig.com and kundenservice@vig.com, bounced outright (mailer-daemon, address not found) and were dropped from every subsequent message.

Nine further follow-ups were sent over the next 78 days, on 6 July, 17 July, 23 July, 31 July, 9 August (two separate sends, one of which again attempted and again lost presse@vig.com), 21 August, 28 August, and 12 September 2026, each restating the same three open questions verbatim: whether Bloomreach/Exponea is entered in VIG health insurance's Art. 30 record of processing activities, whether the open attribution configuration was assessed in an Art. 35 data protection impact assessment, and whether a documented, proportionate purpose exists for continuous background location access after device boot.

Across this entire record, spanning ten messages to the same two mailboxes over 78 days, no reply of any kind, not even an automated ticket acknowledgment, was ever received from datenschutz@vig.com or security@vig.com. The stated embargo of 26 September 2026 passed 21 days before this report's publication, with the correspondence record unchanged since 12 September.

Findings

B1: Exponea/Bloomreach customer data platform embedded in a health-insurance claims app

CRITICAL (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) — Art. 9 health-usage data routed into a marketing-automation platform with no identified legal basis

```
com/exponea/sdk/database/      -- local event database
com/exponea/sdk/network/      -- transmission to Exponea servers
com/exponea/sdk/telemetry/    -- usage telemetry
com/exponea/sdk/manager/      -- campaign management
com/exponea/sdk/models/       -- customer profile models
com/exponea/sdk/services/     -- background services
com/exponea/sdk/view/         -- in-app messaging UI
res/xml/exponea_default_backup_rules.xml (+ _v12 variant)
```

Vendor: Exponea / Bloomreach Engagement, Brno, Czech Republic
Infrastructure: AWS (US) and other US providers

Impact: The VIG KV App ships the complete Exponea SDK (now Bloomreach Engagement) with its own local event database, network layer, telemetry, campaign-management, customer-profile models, background services, and in-app-messaging UI (small packages confirmed: com/exponea/sdk/database/, network/, telemetry/, manager/, models/, services/, view/). On a health-claims app, usage behavior while opening a claim, viewing a benefits statement, uploading a physician document, or browsing medication information is ingested into a marketing-automation engine that builds persistent customer profiles for campaign targeting and push messaging. Exponea is headquartered in Brno, Czech Republic, with cloud infrastructure on AWS and other US providers. GDPR Art. 9(2) requires an explicit legal basis for processing health data for a purpose like this; none is identifiable in VIG's published privacy notice. Art. 13 requires disclosure of this recipient; Art. 44 governs the resulting third-country transfer.

B2: Privacy Sandbox advertising-attribution data opened to every app on the device

CRITICAL (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9) — install/open attribution for a private health-insurance app readable by any co-installed app, blast-radius escalated from MEDIUM

```
res/xml/ga_ad_services_config.xml:  
<ad-services-config>  
  <attribution allowAllToAccess="true"/>  
</ad-services-config>
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM to CRITICAL because the data exposed is not generic ad-attribution noise but a proxy signal for active private health-insurance shopping. `res/xml/ga_ad_services_config.xml` sets `<attribution allowAllToAccess="true"/>` in the Android Privacy Sandbox Attribution API, meaning any other app installed on the same device can read which advertising campaign led to the VIG KV App's install or open. For a private health-insurance app specifically, the fact that a person is actively researching or installing this category of app is itself an indirect indicator of health-consciousness, anticipated illness, or employment change, exactly the kind of inference GDPR Art. 5(1)(c) data minimisation and Art. 13 transparency are meant to constrain, and `allowAllToAccess="true"` removes any restriction on which app can read it.

B3: Production Google Cloud API key hardcoded in the release binary

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N, 7.1) — quota-exhaustion denial-of-service against VIG's own geo services, blast-radius escalated from MEDIUM

```
res/values/strings.xml:  
gcp_apikey_geo = AIzaSyDcE1mZjlfN0FYaSU5irbohZFGy1d2Vnpo
```

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM to CRITICAL because a health-insurance app's mapping/location features (claims office lookup, in-network provider search) failing outright for all users is a direct availability harm, not a theoretical exposure. `res/values/strings.xml` stores `gcp_apikey_geo = AIzaSyDcE1mZjlfN0FYaSU5irbohZFGy1d2Vnpo` in plaintext, readable by anyone who downloads the Play Store binary. An attacker can script bulk calls against Google's Geo/Maps/Places/Geocoding APIs using this key, exhausting VIG's Google Cloud quota and causing legitimate map and location features in the app to fail, with the cost and outage landing on VIG. Art. 32 GDPR requires appropriate technical security measures; a plaintext production credential in a public binary does not meet that bar.

H1: Boot-triggered autostart combined with precise location access, no documented purpose

HIGH (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.5)
 — continuous background-location capability on a claims-and-benefits app with no identified use case

```
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED
uses-permission: android.permission.ACCESS_FINE_LOCATION
uses-permission: android.permission.ACCESS_COARSE_LOCATION
<receiver android:name="androidx.work.impl.background.systemalarm.RescheduleReceiver">
  <intent-filter><action android:name="android.intent.action.BOOT_COMPLETED"/></intent-filter>
</receiver>
```

Impact: The app declares RECEIVE_BOOT_COMPLETED and registers androidx.work.impl.background.systemalarm.RescheduleReceiver against that action, so it restarts automatically after every device reboot, while separately holding ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION. VIG KV App's core functions are claims submission, benefits overview, and document management; no feature requiring continuous or boot-triggered precise-location capture is identifiable, and no explicit consent evidence for background location tracking was found in the binary. GDPR Art. 5(1)(c) data minimisation and Art. 7 valid-consent requirements both apply.

Impact Analysis

VIG KV App is a case where a genuinely better-than-average security baseline, certificate transparency enforcement, biometric authentication, a modern Compose architecture, co-exists with a categorical data-governance problem: a full third-party marketing-automation platform sitting directly on top of health-claims usage data, with no identifiable Art. 9(2) legal basis. B2 and B3 are not exotic; they are the kind of configuration-default and credential-hygiene issues that show up across this research series, but B2 specifically carries elevated weight here because the app category itself, private health insurance, turns an ordinary ad-attribution leak into a health-status inference channel.

The correspondence failure is unusually complete. Ten messages over 78 days to datenschutz@vig.com and security@vig.com, the two addresses that survived VIG's own CC list after presse@vig.com and kundenservice@vig.com bounced on message one, produced not a single reply of any kind, not even an automated acknowledgment. That is a flatter silence than most targets in this series, where at minimum a ticket bot usually fires.

The Complete Chain: Ten Messages, Two Surviving Mailboxes, Zero Replies Of Any Kind, 108 Days

Step 1, Disclosure sent, two CC bounces: RFI-IRFOS sends the original 3 Critical / 1 High findings to datenschutz@vig.com and security@vig.com on 26 June 2026, CC presse@vig.com and kundenservice@vig.com, BCC the Austrian Datenschutzbehörde and Finanzmarktaufsicht, stating a 26 September 2026 embargo. Both CC addresses bounce outright and are dropped from the distribution list for every subsequent message.

Step 2, Eight further follow-ups: 6 July, 17 July, 23 July, 31 July, 9 August (two separate sends), 21 August, and 28 August 2026, each restating the same three open questions to the same two surviving addresses. The 9 August follow-up again attempts presse@vig.com and again bounces.

Step 3, Ninth message, 78 days: On 12 September 2026, RFI-IRFOS sends the ninth message in the thread, again restating all three questions verbatim and noting that no response of any kind, human or automated, has been received since the original disclosure.

Step 4, Embargo reached, then passed: The stated embargo of 26 September 2026 passes with the correspondence record unchanged: ten RFI-IRFOS messages, two permanently bounced CC addresses, zero replies of any kind from either addressed mailbox.

Step 5, Publication: This report publishes 21 days after the embargo date, on the terms stated from the first message.

Across 108 days and two directly-addressed mailboxes at an ATX-listed insurance group, with the Austrian DSB and FMA in BCC from the first message, not one reply of any kind was ever produced to a disclosure naming health-claims data flowing into a marketing-automation platform.

Data Protection — Article by Article

Art. 9(2) GDPR, processing of special-category health data: B1's routing of claims, benefits, document-upload, and medication-browsing behavior into the Exponea/Bloomreach customer data platform requires an explicit Art. 9(2) legal basis; none is identifiable in VIG's published privacy notice.

Art. 13(1)(e) GDPR, recipients of personal data: B1's Exponea/Bloomreach recipient and B3's exposed GCP project are both undisclosed recipients/processors Art. 13 requires to be named.

Art. 5(1)(c) GDPR, data minimisation: B2's allowAllToAccess="true" attribution exposure and H1's boot-triggered precise-location access both collect or expose more than the stated purpose requires.

Art. 44 GDPR, third-country transfers: B1's AWS/US infrastructure behind a Brno, Czech Republic vendor constitutes a third-country transfer of health-adjacent usage data requiring a documented Art. 44 safeguard.

Art. 7 GDPR, conditions for consent: H1's background location capture has no identified explicit consent evidence in the binary.

Art. 32(1)(a) GDPR, security of processing: B3's hardcoded production API key is a release-hardening failure inconsistent with the technical measures Art. 32 requires.

Regulatory & Legal Landscape

Vienna Insurance Group AG is listed on the Vienna Stock Exchange (ATX: VIG); its health-insurance operations are subject to supervision by both the Austrian Datenschutzbehörde (DSB) for data protection and the Finanzmarktaufsicht (FMA) for insurance-sector conduct. Both authorities were BCC'd on this disclosure from the first message onward.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 9 special-category processing issue in B1 and the Art. 13 transparency issues in B1 and B3, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 32 security-of-processing issue in B3, up to EUR 10,000,000 or 2% of total worldwide annual turnover. That ten messages to two directly-addressed mailboxes at an ATX-listed, FMA-supervised insurer, with both national regulators in BCC throughout, produced zero responses of any kind across 108 days is itself a fact relevant to any regulator assessing institutional engagement with a disclosed Art. 9 finding.

Indicators of Compromise

The following SDK packages, configuration values, and credentials were extracted from the production APK (v5.4.2, versionCode 1017216) via static analysis only. No VIG servers, accounts, or infrastructure were probed, and no account was created.

```
B1 -- com/exponea/sdk/{database,network,telemetry,manager,models,
    services,view}/, res/xml/exponea_default_backup_rules(.xml, _v12.xml)

B2 -- res/xml/ga_ad_services_config.xml: allowAllToAccess="true"

B3 -- res/values/strings.xml: gcp_apikey_geo =
    AIzaSyDcE1mZj1fn0FYaSU5irbohzFGy1d2Vnpo

H1 -- AndroidManifest.xml: RECEIVE_BOOT_COMPLETED, ACCESS_FINE_LOCATION,
    ACCESS_COARSE_LOCATION, RescheduleReceiver/BOOT_COMPLETED
```

Disclosure Timeline & Outcome

2026-06-26 Initial disclosure sent to datenschutz@vig.com and security@vig.com, CC presse@vig.com and kundenservice@vig.com, BCC DSB and FMA. Both CC addresses bounce permanently and are dropped.

2026-07-06, 07-17, 07-23, 07-31 Four follow-ups to the two surviving addresses, restating the three open questions. No reply of any kind to any of them.

2026-08-09 Two separate follow-up sends; presse@vig.com attempted again and bounces again. No reply.

2026-08-21, 08-28 Two further follow-ups. No reply.

2026-09-12 Ninth message in the thread, 78 days since disclosure, all three questions restated verbatim. No reply.

2026-09-26 Stated embargo date reached. Correspondence record: ten RFI-IRFOS messages, two permanently bounced addresses, zero replies of any kind.

2026-10-17 This report published, 21 days after the embargo date. All four findings confirmed unaddressed on the basis of the correspondence record.

Residual Risk & Recommendations

B1 – Immediate: Establish and document an Art. 9(2) legal basis for routing health-claims usage behavior into Exponea/Bloomreach, or remove health-adjacent event tracking from the SDK's scope. Enter Bloomreach Inc./Exponea in the Art. 30 record of processing activities if not already present.

B2 – Immediate: Set `allowAllToAccess="false"` (or an explicit allow-list) in the Privacy Sandbox Attribution configuration, and document whether this configuration was assessed in an Art. 35 DPIA.

B3 – Immediate: Rotate the exposed GCP API key, restrict it by package/certificate fingerprint and API scope, and audit for abuse.

H1 – Near-term: Remove `ACCESS_FINE_LOCATION` and the boot-triggered autostart unless a specific, disclosed, and proportionate purpose is documented and consented to separately from general app permissions.

Across all findings: establish a monitored path for security and data-protection disclosures that produces at minimum an automated acknowledgment. Over 108 days and ten messages, neither datenschutz@vig.com nor security@vig.com, the two mailboxes an ATX-listed insurer's own domain designates for exactly this purpose, produced any response at all to a disclosure naming Art. 9 health data flowing into a marketing-automation platform.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static root-level analysis of

the published application using publicly available tooling. No VIG servers, accounts, or infrastructure were probed, and no account was created. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF VIG-KVAPP-2026.