Coordinated Privacy Disclosure, Final Report

winkk AI Android (ai.winkk.app.winkkai)

winkk (Jakob Stadlhuber), Austria

GENUINE TECHNICAL ENGAGEMENT, ONE LEGAL THREAT NEVER ENFORCED, THEN SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE ORIGINAL EMBARGO DATE

Target	winkk AI, an identity/authentication-platform Android app
Package	ai.winkk.app.winkkai
Operator	winkk, represented in correspondence by co-founder Jakob Stadlhuber
Initial Disclosure	2026-06-27
Original Embargo	2026-09-25 (90 days from disclosure, as stated in the original notice and reconfirmed explicitly on 9 July 2026)
Report Published	2026-09-25, on the original embargo date
Regulators	Austrian DSB, European Data Protection Supervisor (EDPS)
Total Outbound Messages	9, across 71 days, to office@winkk.com, support@winkk.ai, and, from R4 onward, jakob@winkk.com directly.
Inbound Replies	2 substantive, technical replies from co-founder Jakob Stadlhuber (9 July 2026, twice), disputing specific findings point by point, followed by a 7-day legal-removal demand the same day; the deadline passed on 16 July 2026 without any legal action being taken. No further reply was received after 9 July 2026.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to winkk that its Android app's compiled Dart runtime (libapp.so) contains a hardcoded PostHog API key and a US-region host (us.i.posthog.com), alongside a Sentry ContentProvider (SentryPerformanceProvider) declared with initOrder=200, meaning it initializes before Application.onCreate() and before any consent mechanism could run, the only ContentProvider in the app's manifest carrying an explicit initOrder among six total. Co-founder Jakob Stadlhuber replied on 9 July 2026 disputing three points: that PostHog data goes to a US host, not Europe (asserting instead that requests go to "PostHog Europe"), that a Sentry DSN could be used to read error logs, and that the persistent microphone background service was a hallucination.

RFI-IRFOS re-pulled the full production bundle, base APK plus the native arm64-v8a library, the same day, confirming the PostHog host and API key were unchanged and that RECORD_AUDIO, FOREGROUND_SERVICE_MICROPHONE, and a boot-restart receiver for the microphone service were all still present exactly as reported. On the Sentry DSN, RFI-IRFOS accepted the correction: a Sentry DSN is architecturally a client-embedded, write-only identifier, not a read scope, and the original description overstated this; the finding was corrected to reflect that an unrestricted, hardcoded DSN allows fabricated event injection into winkk's own Sentry project, not log exfiltration, and its severity was revised down accordingly. Mr. Stadlhuber issued a 7-day deadline the same day demanding removal of the public findings, citing reputational harm; that deadline passed on 16 July 2026 without any legal action taken, and no further reply was received after 9 July 2026 despite three further follow-ups.

A subsequent, independent re-audit conducted the same day, going beyond the scope of the original review, found a finding materially stronger than any originally reported: winkk's own privacy policy states PostHog is used "in Europe" and "collects no data from end-users," and Google Play's Data Safety sheet states no data is shared with third parties. The compiled binary contains a full PostHog session-replay module (screen and touch capture), a touch-autocapture integration, and a complete in-app survey module, all wired to a live, non-empty API key against the same US-region host already confirmed, and the SDK's own bundled code confirms it only disables itself when the key is empty, which it is not. Nine messages were sent in total across 71 days. The 90-day embargo, reconfirmed explicitly in writing on 9 July 2026, elapses today, 25 September 2026, and this report publishes on that date.

Scope: Root-level static analysis of the production winkk AI Android application (ai.winkk.app.winkkai, version 1.4.0), reviewed initially on 27 June 2026 and independently re-verified against a freshly pulled, byte-identical production bundle (base.apk plus the arm64-v8a native library) on 9 July 2026, following the target's dispute of specific findings. No dynamic instrumentation, live network capture, or interaction with winkk's or PostHog's backend infrastructure was performed; the question of whether a live PostHog event actually left the device at runtime remains outside the scope of this static analysis.

Disposition

This case involved genuine, substantive technical back-and-forth, not silence or automated deflection. winkk's co-founder disputed three specific points on 9 July 2026; RFI-IRFOS independently re-pulled the full production bundle the same day and confirmed two of the three disputed points stood exactly as reported, while accepting and correcting a real overstatement in its own description of the third (a Sentry DSN's technical capabilities). A subsequent, more thorough re-audit went further than the original scope and found a fourth, independently stronger finding: the app's own privacy policy and Google Play Data Safety sheet make specific, falsifiable claims about PostHog ("Europe-based," "collects no data from end-users") that are directly contradicted by a fully-featured PostHog session-replay, touch-autocapture, and survey module compiled into the binary and wired to a live, non-empty API key against a US-region host. This finding reaches HIGH on the computed CVSS score alone. A pre-consent Sentry ContentProvider and an unrestricted Sentry DSN correct to MEDIUM; a persistent microphone background service corrects to LOW. A 7-day legal-removal demand was issued on 9 July 2026 and never enforced.

ID	Severity	Title
N1	HIGH	Privacy Policy and Play Data Safety Sheet Contradict a Fully-Featured PostHog Session-Replay Module Compiled Into the Binary
H1	MEDIUM	Sentry ContentProvider Initializes Before Application.onCreate(), the Only Provider With an Explicit initOrder
H2	MEDIUM	Unrestricted Sentry DSN Hardcoded, Allowing Fabricated Event Injection
H3	LOW	Persistent Microphone Background Service Tied to a Boot-Restart Receiver

Subject & Operator Analysis

winkk AI is an identity and authentication-platform Android app. This case is unusual in this campaign for the depth of genuine technical engagement received: co-founder Jakob Stadlhuber replied twice on 9 July 2026 with specific, substantive technical counter-arguments, not a form deflection or a boilerplate acknowledgment.

Several genuine positives are worth naming, including a real, credited correction on RFI-IRFOS's own side: the original Sentry DSN finding overstated its capability, and that was corrected in writing during the exchange, not silently. targetSdkVersion=36 correctly defaults cleartext HTTP to blocked with no override found. No Chinese, Russian, or other unexpected third-country SDKs were found anywhere in an exhaustive sweep of both the compiled Dalvik bytecode and the native library. Several other leads (a suspicious-looking string resembling a PostHog proxy domain, a Stripe publishable key) were chased and explicitly ruled out, not padded into findings they were not.

Genuine Technical Dispute, a Legal Threat, and Then Silence

This case's correspondence record includes real, substantive technical engagement, not silence or automated deflection. Following two prior unanswered follow-ups, Jakob Stadlhuber replied on 9 July 2026 disputing three specific points. RFI-IRFOS re-pulled the complete production bundle the same day and replied point by point: two disputed points, the PostHog host and the microphone background service, were confirmed unchanged against the freshly pulled binary; the third, the Sentry DSN's capabilities, was found to be a genuine overstatement in RFI-IRFOS's own original wording and was corrected in writing, with the finding's severity revised down accordingly. Separately, on the same day, a 7-day deadline was issued demanding removal of the public findings, citing reputational harm and referencing archived material for possible legal action; that deadline passed on 16 July 2026 without any legal action being taken. Three further follow-ups, through 6 September 2026, restated the same three outstanding questions and drew no further reply of any kind.

Findings

N1: Privacy Policy and Play Data Safety Sheet Contradict a Fully-Featured PostHog Session-Replay Module Compiled Into the Binary

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. Kept deliberately conservative: live network transmission of a specific event was not dynamically confirmed in this pass, only that the collecting code is present, configured, and not in a disabled state per the SDK's own logic.

winkk's own privacy policy (§6.3.2, independently fetched and re-verified via direct HTTP request) states that PostHog is used "in Europe" and "collects no data from end-users." Google Play's Data Safety sheet for this package, independently fetched the same way, states "no data shared with third parties." The compiled binary contains a complete PostHog session-replay module (RRWireframe, RRFullSnapshotEvent, RRIncrementalSnapshotEvent, RRMouseInteraction, a dedicated PostHogReplayThread and on-disk replay queue), a touch-autocapture integration (PostHogTouchActivityIntegration), and a full in-app survey module, all configured against us.i.posthog.com, not eu.i.posthog.com, with a live, non-empty API key. The SDK's own bundled log string states it disables itself only when the key is empty after trimming whitespace, which, per the key confirmed present, it is not.

```
PostHog session-replay classes: RRWireframe, RRFullSnapshotEvent,
    RRIncrementalSnapshotEvent, RRMouseInteraction, PostHogReplayThread
PostHogTouchActivityIntegration (touch/UI autocapture), com/posthog/surveys/* (in-app
    surveys)
Configured host: us.i.posthog.com (confirmed, not eu.i.posthog.com)
SDK log string: "PostHog SDK is disabled because the API key is required and was empty
     after trimming whitespace." (key present, non-empty)
```

Impact: A specific, quotable, falsifiable claim in a formal legal document (the privacy policy) and a formal platform disclosure (Play Data Safety) is difficult to reconcile with shipping a session-replay-capable, autocapture-capable, survey-capable client wired to a live key against a US host; the collecting code is present and active by the vendor's own enablement logic.

Fix: Correct the privacy policy and Play Data Safety sheet to accurately reflect the PostHog configuration actually shipped, or reconfigure PostHog to match the stated EU-only, no-data-collection claim. No confirmation that this has occurred was ever received.

H1: Sentry ContentProvider Initializes Before Application.onCreate(), the Only Provider With an Explicit initOrder

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. Confirmed unchanged on independent re-verification, 9 July 2026, following the target's dispute.

SentryPerformanceProvider is declared with initOrder=200, confirmed via aapt2 manifest analysis. Of six total ContentProviders in the manifest, this is the only one carrying an explicit initOrder; the other five are benign platform/plugin infrastructure (clipboard, file providers, androidx startup). No consent-management-platform class of any kind (OneTrust, Didomi, Usercentrics, IAB TCF) exists anywhere in the compiled code, and an exhaustive string search found no consent-dialog copy in either English or German beyond a bare unrelated PostHog API method name.

```
io.sentry.android.core.SentryPerformanceProvider, initOrder=200 (only provider in the
    manifest with an explicit initOrder)
```

Impact: Sentry performance monitoring begins before Application.onCreate() runs, and no technical consent mechanism exists anywhere in the app to gate it or any other collection.

Fix: Defer SentryPerformanceProvider initialization until after an app-native consent flow has run, and implement a genuine consent-management platform. No confirmation that this has occurred was ever received.

H2: Unrestricted Sentry DSN Hardcoded, Allowing Fabricated Event Injection

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9. Severity corrected downward from the original disclosure following winkk's own dispute: a Sentry DSN is a write-only client identifier, not a read scope, and cannot be used to exfiltrate existing logs, as the original wording incorrectly implied. This correction is made in the interest of accuracy, not because the underlying finding was withdrawn.

The full Sentry DSN, https://a5e7fbb064331d0fee60519ed4a22223@sentry.winkk.dev/45, is confirmed hardcoded in libapp.so. A Sentry DSN is architecturally a client-embedded, write-only identifier; it cannot be used to read existing error logs, a point winkk correctly raised and RFI-IRFOS accepted. What remains accurate: an unrestricted, hardcoded DSN allows anyone who extracts it to inject fabricated events into winkk's own Sentry project, independent of whether the embedding itself is standard practice.

```
https://a5e7fbb064331d0fee60519ed4a22223@sentry.winkk.dev/45 (public key
    a5e7fbb064331d0fee60519ed4a22223, host sentry.winkk.dev, project id 45, confirmed
    an on-premises Sentry deployment per winkk's own privacy policy §6.2.1)
```

Impact: Anyone who extracts the DSN could inject fabricated events into winkk's own Sentry project; this does not expose existing log data, correcting the original disclosure's overstated claim.

Fix: Rate-limit or rotate the DSN if fabricated event injection is a concern for this deployment. No confirmation that this has occurred was ever received.

H3: Persistent Microphone Background Service Tied to a Boot-Restart Receiver

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4. Confirmed unchanged on independent re-verification, 9 July 2026, following the target's dispute that this was a hallucination.

RECORD_AUDIO, FOREGROUND_SERVICE_MICROPHONE, and RECEIVE_BOOT_COMPLETED are all declared, alongside a registered BOOT_COMPLETED/QUICKBOOT_POWERON receiver (com.pravera.flutter_foreground_task.service.RestartReceiver) whose sole documented purpose, per its own plugin documentation, is restarting the foreground microphone service after a device reboot.

```
android.permission.RECORD_AUDIO, FOREGROUND_SERVICE_MICROPHONE, RECEIVE_BOOT_COMPLETED
com.pravera.flutter_foreground_task.service.RestartReceiver (BOOT_COMPLETED/
    QUICKBOOT_POWERON)
```

Impact: A microphone-capable foreground service is configured to automatically restart after every device reboot; the practical exploitation path and actual runtime trigger conditions require dynamic analysis the static review could not perform, which keeps the computed score low.

Fix: Document the specific feature requiring persistent, boot-surviving microphone access. No confirmation that this has occurred 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. 5(1)(a), Art. 12, Art. 13	N1	Privacy policy and platform disclosure contradicting the compiled PostHog configuration.
Art. 7, Art. 25	H1	Pre-consent Sentry ContentProvider initialization, no consent mechanism exists at all.
Art. 32	H2	Unrestricted, hardcoded Sentry DSN allowing fabricated event injection.
Art. 5(1)(c), Art. 13(1)(c)	H3	Undocumented, boot-persistent microphone background service.

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. In this report, N1 reaches HIGH on its computed CVSS v4.0 score alone, no editorial escalation applied; H1 and H2 correct to MEDIUM to match their own computed bands, with H2's severity specifically revised downward following a correction RFI-IRFOS accepted from winkk during the exchange; H3 corrects to LOW on its own computed band. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: WINKK-2026-R1.