Coordinated Security & Privacy Disclosure, Final Report

Vlad and Nikita for Android (me.apptivise.vladnikita, v2.8.0)

Thirteen written notices, eighty-eight days, zero replies of any kind, a children's app with a 100 million-plus subscriber audience

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FIVE FINDINGS UNADDRESSED AFTER THIRTEEN NOTICES, ZERO REPLIES

Target	Mobinautica Limited, Cyprus
Product audited	Vlad and Nikita for Android, me.apptivise.vladnikita, v2.8.0 (companion app to the Vlad and Nikita children's YouTube channel, 100 million-plus subscribers)
Disclosure reference	REF RFI-2026-MB-001
R1 sent	2026-06-24
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 microphone and camera access in a toddler-targeted app with no verifiable parental consent mechanism anywhere in the app flow, CVSS v4.0 8.7, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 24 June 2026, RFI-IRFOS performed static analysis of the production Vlad and Nikita Android application, the companion app to a children's YouTube channel with over 100 million subscribers and a target audience aged 2 to 6, and identified three CRITICAL and two HIGH findings: RECORD_AUDIO and CAMERA permissions declared and requested with no consent gate on first launch and no privacy notice shown before the permissions are requested, meaning toddlers' voice recordings, biometric data under GDPR Art. 9(1), may be captured with no verifiable parental consent mechanism anywhere in the app, 831 references to IMEI and TelephonyManager APIs across the decompiled bytecode, indicating persistent hardware-identifier collection from a device primarily used by a child with no consent, disclosure, or documented lawful basis, a 396-class WeChat SDK (Tencent, PRC jurisdiction, no EU adequacy decision under Art. 46) and a 2,895-class Facebook SDK, both undisclosed as data processors in the privacy policy with no Art. 28 processing agreement referenced, two distinct hardcoded Firebase API keys in the production binary, suggesting either a multi-project Firebase setup or an incomplete key rotation, and a published privacy policy that names only a Gmail address as its sole data-subject contact, disclosing no DPO, no legal entity name, and no registered address, falling short of GDPR Art. 13's minimum transparency requirements.

Across thirteen written notices over eighty-eight days, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde, the German BfDI, the Cypriot Commissioner for Personal Data Protection, CERT.at, and the EDPS, not one reply of any kind, automated or human, was ever received from Mobinautica Limited or any address associated with it. None of RFI-IRFOS's six standing questions, on DPO awareness, a documented Art. 8 parental-consent mechanism, the Art. 6/8 lawful basis for microphone and camera activation, the Art. 46 transfer mechanism for data routed to China, or Art. 33/35 regulatory notification and DPIA status, ever received an answer.

Scope: Static analysis of the publicly downloaded production Vlad and Nikita Android APK (v2.8.0), on an authorized test device, only. No Mobinautica account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 24 June 2026 to mobinautica@gmail.com, cc a second Mobinautica-linked address, bcc the Austrian Datenschutzbehoerde, the German BfDI, the Cypriot Commissioner for Personal Data Protection, CERT.at, and the EDPS. Across thirteen written notices over eighty-eight days, not one reply of any kind, automated or human, was ever received from Mobinautica Limited or any address associated with it.

ID	Severity	Title
C1	CRITICAL	RECORD_AUDIO and CAMERA in a toddler-targeted app with no verifiable parental consent mechanism
C2	CRITICAL	831 IMEI/TelephonyManager references – persistent device identifier collection from children's devices

ID	Severity	Title
C3	CRITICAL	WeChat and Facebook SDKs – undisclosed PRC and third-country transfers
H1	HIGH	Two hardcoded Firebase API keys in the production binary
H2	HIGH	Privacy policy names only a Gmail address, no DPO, legal entity, or registered address

Subject & Operator Analysis

Mobinautica Limited, Cyprus, operates the companion app for the Vlad and Nikita children's YouTube channel, one of the largest children's media properties on the platform with over 100 million subscribers. The privacy policy itself does not name this entity; it was identified from correspondence and app-store listing metadata.

Findings

C1: RECORD_AUDIO and CAMERA in a toddler-targeted app with no verifiable parental consent mechanism

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

AndroidManifest.xml declares android.permission.RECORD_AUDIO and android.permission.CAMERA in production. The app's target audience is children aged 2-6, matching the Vlad and Nikita YouTube channel's own content. No consent gate exists on first launch, and no privacy notice is shown before these permissions are requested.

Voice recordings of toddlers constitute biometric data under GDPR Art. 9(1), and no verifiable parental consent mechanism exists anywhere in the app flow. No reply of any kind addressed this finding across thirteen notices.

Impact: Children's voice and image data may be captured with no consent gate and no verifiable parental consent mechanism of any kind, on an app serving one of the largest children's media brands on the platform.

Fix: Implement a verifiable parental-consent gate before requesting microphone or camera permissions, and display a privacy notice before any such permission request.

C2: 831 IMEI/TelephonyManager references – persistent device identifier collection from children's devices

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

Static analysis found 831 references to getDeviceId, IMEI, and TelephonyManager across the decompiled bytecode. IMEI is a persistent hardware identifier enabling cross-session and cross-app tracking.

This identifier is collected from a device primarily used by a child, with no consent, disclosure, or documented lawful basis. No reply of any kind addressed this finding.

Impact: A persistent hardware identifier tied to a child's device enables long-term cross-app tracking with no consent mechanism or disclosed purpose.

Fix: Remove IMEI/device-ID collection unless a specific, disclosed, and consented purpose requires it, and use resettable identifiers instead.

C3: WeChat and Facebook SDKs – undisclosed PRC and third-country transfers

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 binary contains 396 smali classes from Tencent's WeChat SDK (com/tencent/ namespace, PRC jurisdiction, no EU adequacy decision under Art. 46) and 2,895 smali classes from Facebook's SDK. Both are undisclosed as data processors in the privacy policy, and no Art. 28 processing agreement is referenced for either.

No reply of any kind addressed whether either transfer has a documented Art. 46 mechanism.

Impact: Children's app data may be transferred to a PRC-jurisdiction recipient and to a US recipient with no disclosed processor relationship or transfer mechanism for either.

Fix: Name WeChat/Tencent and Facebook explicitly as processors, document Art. 28 agreements, and cite the Art. 46 transfer mechanism for the PRC-jurisdiction recipient.

H1: Two hardcoded Firebase API keys in the production 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

Two distinct hardcoded Firebase API keys, AIzaSyAfNfevB5fSH3QJ_q0_lC8mlMfKdVj0fIw and AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE, are extractable from the APK without root or specialist tooling, suggesting either a multi-project Firebase setup or an incomplete key rotation.

No reply of any kind addressed this finding.

Impact: Two separate Firebase projects' attack surfaces cannot be independently ruled safe from outside the console once both keys ship in every installed client.

Fix: Rotate both keys, consolidate to a single project if the second is a leftover from migration, and restrict each key to the correct package name and signing fingerprint.

H2: Privacy policy names only a Gmail address, no DPO, legal entity, or registered address

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

The published privacy policy lists mobinautica@gmail.com as the sole data-subject contact. It does not name a Data Protection Officer, does not disclose the legal entity name (Mobinautica Limited), does not provide a registered address, and does not identify Cyprus as the place of establishment.

No reply of any kind addressed this finding.

Impact: Data subjects, including parents seeking to exercise rights on behalf of a child, have no way to identify the actual controller or a functional escalation path beyond a Gmail address.

Fix: Name the legal entity, registered address, place of establishment, and, if required, a Data Protection Officer in the privacy policy.

Thirteen Notices, Zero Replies, A 100 Million-Subscriber Audience

Across thirteen written notices sent over eighty-eight days on a single continuous thread, not one reply of any kind, automated or human, was ever received from Mobinautica Limited or any address associated with it. This is the only case in this disclosure wave where a target with an audience of this scale, a children's brand exceeding 100 million subscribers, produced total silence across every single notice.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 8, Art. 9(1)	Microphone/camera access on a toddler app with no consent mechanism
C2	GDPR Art. 5(1)(b)(c), Art. 6	Persistent device-ID collection from children's devices
C3	GDPR Art. 13(1)(e), Art. 28, Art. 46	Undisclosed PRC and US transfers via WeChat and Facebook SDKs
H1	GDPR Art. 25(1), Art. 32(1)(b)	Two hardcoded Firebase keys, possible incomplete rotation
H2	GDPR Art. 13	Privacy policy fails minimum transparency requirements

Disclosure Timeline & Outcome

Date	Event
2026-06-24	R1 sent to mobinautica@gmail.com; 3 CRITICAL + 2 HIGH findings; bcc Austrian DSB/German BfDI/Cypriot C ommissioner/CERT.at/EDPS; a EUR 4,500 confidential engagement figure was referenced under the R1 policy then in force – historical record only, not a currently open offer
2026-06-27	Follow-up, three days no reply; a EUR 9,000 confidential figure referenced under the same then-current policy – also historical only
2026-06-30	72-hour sweep sent, six days silence, three questions restated
2026-07-03	Follow-up, nine days silence, Austrian DSB and EDPS moved from bcc to open cc
2026-08-21	Follow-up, fifty-eight days silence
2026-09-11	Follow-up, seventy-nine days since disclosure, zero replies, embargo in eight days
2026-09-16	Follow-up, day 84, zero replies to six substantive messages, embargo in three days, weekly SHA-256 diffing during the embargo period disclosed
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Implement a verifiable parental-consent gate before any microphone or camera permission request.
- Remove persistent device-identifier (IMEI) collection unless a specific, disclosed, consented purpose requires it.
- Name WeChat/Tencent and Facebook explicitly as processors, with documented Art. 28 agreements and the Art. 46 transfer mechanism for the PRC-jurisdiction recipient.
- Rotate both exposed Firebase keys.
- Complete the privacy policy with the legal entity name, registered address, and a functional contact beyond a Gmail address.

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. 5, 6, 8, 9, 13, 25, 28, 32, 46. REF RFI-2026-MB-001.