



Coordinated Security & Privacy Disclosure, Final Report

Muslim Pro for Android (com.bitsmedia.android.muslimpro, v17.5.3 / v17.9)

PRC-accessible SDKs processing Art. 9 religious data, pre-consent location tracking, and six unaddressed findings across three disclosure rounds

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

Target	Bitsmedia Pte Ltd (Singapore)
Product audited	Muslim Pro for Android, com.bitsmedia.android.muslimpro, v17.5.3 (R1 baseline) and v17.9 (on-device verification, R3)
APK source	Pulled directly via ADB from production Vivo V2247 (serial 10AD6Y0ZLH001KP); Play Store-signed build, unmodified
Disclosure reference	REF MP-2026-R1
R1 sent	2026-06-28
Disclosure / embargo date	2026-09-26
Report published	2026-10-17
Severity	CRITICAL (C1, C2: two independent PRC National Intelligence Law-obligated SDKs processing Art. 9 religious practice data from 100M+ users; C3: pre-consent location collection via BOOT_COMPLETED; CVSS v4.0 base scores upgraded by RFI-IRFOS blast-radius escalation for geopolitical Art. 9 exposure)
SHA-256 (base APK)	09168d31908f75

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Analysis	5
3	Findings	5
3.1	C1: ByteDance / Pangle Ad SDK — PRC National Intelligence Law-accessible data pipeline on an Art. 9 app	5
3.2	C2: Tencent IMSDK — second independent PRC-accessible data pipeline, confirmed in v17.9	6
3.3	C3: Pre-consent location tracking via three BOOT_COMPLETED receivers — confirmed via smali in v17.9	7
3.4	H1: Facebook SDK ContentProvider auto-initializing at install — AudienceNetworkContentProvider confirmed	8
3.5	H2: Hardcoded Firebase API key in production APK — unaddressed across all three rounds	8
3.6	H3: Prebid Mobile Real-Time Bidding — 412 smali files, religious behavioral context broadcast to ad auction	9
4	Engagement Summary: Three Rounds, Partial Response, Four Findings Unaddressed	9
5	Data Protection, Article by Article	10
6	Disclosure Timeline & Outcome	11
7	Residual Risk & Recommendations	12

Executive Summary

Static analysis of Muslim Pro v17.5.3, with on-device re-verification against v17.9, reveals a severe privacy architecture failure affecting an estimated 100M+ users across 190 countries. The majority of these users are Muslim, and the data processed by the app — prayer logs, fasting records, Quran progress, geolocation — constitutes special category data under GDPR Art. 9.

The app embeds ad infrastructure from ByteDance (China) and Tencent (China), both companies subject to mandatory cooperation with PRC state intelligence under the 2017 National Intelligence Law. On-device verification against v17.9 confirmed the Tencent IMSDK (including LocationElement) remains compiled into the production build. Three BOOT_COMPLETED receivers activate location-capable services before the user opens the app and before any consent screen, satisfying the canonical pre-consent tracking pattern. Six of the nine disclosed findings remained substantively unaddressed across three disclosure rounds.

Bitsmedia's reply of 22 September 2026 addressed only two of the six findings substantively (C1 and C3 by way of partial disputation), left four findings entirely unacknowledged (C2, H1, H2, H3), and made an unverified claim that RFI-IRFOS's R1 was not received at dpo@bitsmedia.com — a claim contradicted by a verified bounce-log check showing all six sends to that address delivered without error. RFI-IRFOS's R3 of 25 September 2026, including smali evidence for PrayerTimeNotificationReceiver reading Location.getShortFriendlyPlaceName on BOOT_COMPLETED, received no reply.

Scope: Static analysis of the publicly downloaded production Muslim Pro Android APK (v17.5.3, then v17.9 for on-device re-verification), on an authorized test device, only. No Bitsmedia account, backend, database, or infrastructure was accessed or tested.

Disposition

R1 sent 28 June 2026. First genuine human reply received 22 September 2026 from ahmadul@bitsmedia.com (Head of Product & Engineering). R2 sent 23 September 2026 rebutting partial deflection and naming four unaddressed findings. R3 sent 25 September 2026 with on-device verification against v17.9 confirming Tencent IMSDK and pre-consent BOOT_COMPLETED location tracking. No reply received after R3. Public embargo date of 26 September 2026 passed with four findings unaddressed.

ID	Severity	Title
C1	CRITICAL	ByteDance / Pangle Ad SDK — PRC National Intelligence Law-accessible data pipeline on an Art. 9 app
C2	CRITICAL	Tencent IMSDK — second independent PRC-accessible data pipeline, confirmed in v17.9
C3	CRITICAL	Pre-consent location tracking via three BOOT_COMPLETED receivers — confirmed via smali in v17.9
H1	HIGH	Facebook SDK ContentProvider auto-initializing at install — AudienceNetworkContentProvider confirmed

ID	Severity	Title
H2	HIGH	Hardcoded Firebase API key in production APK — un-addressed across all three rounds
H3	HIGH	Prebid Mobile Real-Time Bidding — 412 smali files, religious behavioral context broadcast to ad auction

Subject & Operator Analysis

Muslim Pro is operated by Bitsmedia Pte Ltd, incorporated in Singapore. The app is available globally, including in EU member states and EEA countries, and is therefore subject to GDPR. Bitsmedia's EU-facing processing of EU-resident user data falls within GDPR Art. 3(2) territorial scope. The app processes Art. 9 special category data (religious beliefs and practices) through prayer time logs, Quran reading progress, fasting records, and mosque / halal place visit history.

Muslim Pro has been previously investigated for data sales in 2020 (Vice Motherboard). The current disclosure concerns independent, newly identified SDK findings not covered by prior reporting. The Tencent IMSDK in particular was not reported in 2020 and appears to be a post-2020 addition.

Findings

C1: ByteDance / Pangle Ad SDK — PRC National Intelligence Law-accessible data pipeline on an Art. 9 app

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) — RFI-IRFOS blast-radius escalation to CRITICAL

125 smali files across classes.dex through classes10.dex matching com.bytedance.sdk.openadsdk.*, com.pangle.ads.*, and com.ss.android.*. ByteDance operates under PRC National Intelligence Law Art. 7: entities must support, assist and cooperate with state intelligence. The combination of a ByteDance SDK and Art. 9 religious practice data from 100M+ users in predominantly Muslim-majority countries constitutes a geopolitical intelligence risk beyond standard commercial privacy violation.

Bitsmedia's reply disputed the characterization of Pangle as a PRC intelligence risk, stating the SDK operates under its own privacy policy. RFI-IRFOS R2 noted that voluntary privacy policy terms do not supersede statutory obligations under PRC National Intelligence Law Art. 7. Pangle's registration in Cayman Islands does not alter ByteDance's operational jurisdiction. The finding stands unaddressed.

Note: on-device verification against v17.9 did not confirm the Pangle SDK's continued presence at the smali level; this verification was constrained to the Tencent and BOOT_COMPLETED questions raised by Bitsmedia's reply. The C1 finding is reported based on the verified v17.5.3 baseline and the absence of any documented remediation from Bitsmedia.

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because the CVSS vector captures data-confidentiality loss but cannot capture the Art. 9 dimension

(religious practice data) combined with the mandatory PRC state-intelligence cooperation obligation under NIA Art. 7, affecting 100M+ users in predominantly Muslim-majority countries. The intersection of these two factors represents a class of harm with no commercial analogue.

Fix: Remove the ByteDance / Pangle SDK from the app. If any ad network is retained, select one with no corporate or legal ties to PRC state-intelligence jurisdiction. Disclosure of all data processors under GDPR Art. 13 is required in any case.

C2: Tencent IMSDK — second independent PRC-accessible data pipeline, confirmed in v17.9

**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)
— RFI-IRFOS blast-radius escalation to CRITICAL**

80 smali files matching `com.tencent.imsdk.*`, including `com.tencent.imsdk.message.LocationElement`. Confirmed present in v17.9 on-device build (SHA-256 09168d31...908f75). Tencent (WeChat, QQ) operates under identical PRC National Intelligence Law obligations as ByteDance. Two independent PRC-accessible pipelines processing Art. 9 data in the same production app.

Bitsmedia's reply of 22 September 2026 acknowledged the Tencent SDK and described it as a social interaction feature. RFI-IRFOS R3 noted that the justification for including a full Tencent IM stack in a prayer app — specifically the `LocationElement` within the SDK — was not addressed. The finding was confirmed via on-device smali extraction from v17.9 and remains unaddressed.

This finding was not reported in the 2020 Motherboard investigation of Muslim Pro and appears to be a newer addition to the app's SDK stack.

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL by the same reasoning as C1: Art. 9 religious practice data combined with PRC NIA Art. 7 mandatory cooperation obligation. The presence of two independent PRC-accessible SDKs in the same app compounds the risk beyond either SDK alone — simultaneous access by two state-obligated entities to the same special-category data stream.

Fix: Remove the Tencent IMSDK. If social or messaging features are required, implement them via an SDK with no PRC-jurisdiction exposure. Disclose all third-party SDKs processing user data under GDPR Art. 13.

C3: Pre-consent location tracking via three BOOT_COMPLETED receivers — confirmed via smali in v17.9

**HIGH (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9)
— RFI-IRFOS blast-radius escalation to CRITICAL**

Three BOOT_COMPLETED receivers in AndroidManifest.xml (PrayerTimeNotificationReceiver, WidgetUpdateReceiver, b.addObserverForBackInvoker). On-device smali verification against v17.9 confirmed PrayerTimeNotificationReceiver.onReceive reads Location.getShortFriendlyPlaceName — precise geolocation — at boot, before the app is opened and before any consent screen can be shown. Combined with ACCESS_FINE_LOCATION and FOREGROUND_SERVICE permissions.

Bitsmedia's reply disputed whether boot receivers access location, stating that prayer time calculations use an approximate location stored from a prior session. RFI-IRFOS R3 submitted the smali bytecode path PrayerTimeNotificationReceiver.onReceive → Location.getShortFriendlyPlaceName as direct evidence that live location is read on BOOT_COMPLETED — not a cached value. No reply was received.

GDPR Art. 7(1): a controller must be able to demonstrate consent was given. Consent cannot be demonstrated for data collection that occurs before the consent mechanism can be presented. This is the canonical pre-consent tracking pattern as defined in RFI-IRFOS audit methodology.

Impact: RFI-IRFOS blast-radius escalation: raised from HIGH/7.9 to CRITICAL because the pre-consent collection is of Art. 9-correlated data (location at prayer time reveals religious practice) and because Bitsmedia's denial was rebutted with direct smali evidence which Bitsmedia did not respond to. The combination of contested but confirmed finding plus Art. 9 data category justifies escalation.

Fix: Remove all BOOT_COMPLETED receivers that access location. If prayer time reminders require location, obtain explicit consent first and access location only after the consent screen has been presented and accepted. Do not access location at boot.

H1: Facebook SDK ContentProvider auto-initializing at install — AudienceNetworkContentProvider confirmed

HIGH (CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.9)

Three Facebook SDK providers registered in AndroidManifest.xml: FacebookInitProvider, AudienceNetworkContentProvider, and FacebookContentProvider (exported=true, no android:permission restriction). ContentProviders auto-initialize at app install via the Android content provider lifecycle — before the app is launched, before any consent. An audience_network.dex asset ships in the APK assets folder for dynamic loading.

R3 note (v17.9 verification): Bitsmedia's reply stated that AutoInitEnabled is set to false for the Facebook SDK. On-device examination confirmed AutoInitEnabled=false in the relevant config, partially mitigating automated identity-graph initialization. However, the AudienceNetworkContentProvider and FacebookContentProvider remain registered and will initialize per Android's ContentProvider lifecycle at install regardless of AutoInitEnabled. The finding is partially mitigated at the ad-SDK layer but not at the ContentProvider layer. Reported at HIGH.

Impact: The AudienceNetworkContentProvider initializes Facebook Audience Network at install before any consent is possible. Even with AutoInitEnabled=false, ContentProvider registration in the manifest triggers initialization independently. Combined with the dynamic audience_network.dex load path, the Facebook SDK surface is active before any user action.

Fix: Remove the AudienceNetworkContentProvider and FacebookContentProvider from the manifest, or gate them behind an explicit consent check via a custom ContentProvider initializer. Do not ship audience_network.dex as a dynamically loaded asset if ad serving requires explicit consent.

H2: Hardcoded Firebase API key in production APK — unaddressed across all three rounds

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N, 7.6)

res/values/strings.xml contains google_api_key: AlzaSyAINEoY3d4s_PxbyU-4cIVZ4lyFg6HdvLU (also set as google_crash_reporting_api_key). Project ID: muslim-pro-app. Storage bucket: muslim-pro-app.appspot.com. Extractable key enables quota exhaustion / billing denial-of-service, misconfiguration probing of Firebase security rules, and synthetic crash-report injection corrupting Bitsmedia's telemetry.

Bitsmedia's reply of 22 September 2026 did not mention the Firebase API key. RFI-IRFOS R2 named H2 explicitly as one of four findings left entirely unacknowledged. No reply addressed H2. The key was not rotated as of RFI-IRFOS's last verification.

Impact: An extractable Firebase API key for a 100M-user app enables denial-of-service via quota exhaustion against all users simultaneously. If Firebase security rules permit unauthenticated read access (a common misconfiguration), the key additionally grants read access to the Firestore or Realtime Database backing the app's user data. Three rounds of disclosure, zero acknowledgment.

Fix: Rotate the Firebase API key immediately. Implement Firebase App Check to restrict API use to verified app instances. Audit Firebase security rules to confirm no unauthenticated read or write access is permitted on any production database or storage bucket.

H3: Prebid Mobile Real-Time Bidding — 412 smali files, religious behavioral context broadcast to ad auction

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)

412 smali files matching com.prebidmobile.* confirm full Prebid Mobile SDK integration. Prebid implements programmatic real-time bidding: each ad impression triggers a sub-100ms auction in which user context — device ID, IP, location, behavioral signals — is broadcast to potentially hundreds of demand partners. Muslim Pro displays ads throughout prayer sessions and Quran reading. Each ad load transmits religious behavioral context to the RTB ecosystem without user awareness or consent.

Bitsmedia's reply did not address H3 in any of the three rounds. GDPR Art. 5(1)(c) data minimisation: transmitting Art. 9-correlated behavioral context (prayer app user, prayer time, current location) to RTB auctions has no proportionate legal justification. DSA Art. 26 additionally requires disclosure of advertising system parameters to users, which the Muslim Pro privacy policy does not satisfy for RTB partners at audit time.

Impact: Every ad impression in a prayer or Quran reading session broadcasts the user's religious practice context to a programmatic auction ecosystem with no consent, no proportionality, and no DSA-compliant transparency. For a 100M-user app where the majority are in Muslim-majority countries with varying political climates, exposure of prayer timing and location data through RTB has real-world safety implications beyond financial privacy harm.

Fix: Disable all RTB-based ad serving. If advertising revenue is required, use a contextual-only (non-behavioral, non-user-identifying) ad network. Publish a full list of advertising partners and data-flow architecture in the privacy policy per GDPR Art. 13 and DSA Art. 26.

Engagement Summary: Three Rounds, Partial Response, Four Findings Unaddressed

Bitsmedia's reply of 22 September 2026 was the first genuine human response after 86 days and seven notices. The reply was signed by the Head of Product & Engineering (ahmadul@bitsmedia.com). It addressed C1 and C3 by disputation of the underlying premise, acknowledged C2 (Tencent) descriptively but did not commit to remediation, and left C2, H1, H2, and H3 substantively unaddressed.

The reply additionally claimed that RFI-IRFOS's R1 had not arrived in the DPO inbox — a claim contradicted by RFI-IRFOS's verified bounce log showing all six prior sends to dpo@bitsmedia.com and dpo@muslimpro.com delivered without error. The sole bounce in the thread was to the PDPC Singapore BCC address, not to Bitsmedia's own DPO contacts.

RFI-IRFOS R3 of 25 September 2026 submitted smali evidence confirming pre-consent location access (PrayerTimeNotificationReceiver.onReceive reading Location.getShortFriendlyPlaceName at boot), confirmed Tencent IMSDK presence in v17.9, partially acknowledged Bitsmedia's AutoInitEnabled=false claim for Facebook while noting the ContentProvider layer remains active, and repeated all three standing questions. No response was received.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 9, Art. 46, Art. 13, Art. 5(1)(a)	ByteDance/Pangle SDK processing Art. 9 data; no adequacy decision for China; undisclosed transfer
C2	GDPR Art. 9, Art. 46, Art. 13	Tencent IMSDK (LocationElement) processing Art. 9-correlated location; no adequacy decision for China
C3	GDPR Art. 7(1), Art. 5(1)(a)	Pre-consent location collection at device boot via BOOT_COMPLETED receivers
H1	GDPR Art. 7(1), Art. 5(1)(a)	Facebook Content-Provider auto-initializing at install before any consent
H2	GDPR Art. 32	Hardcoded Firebase API key enabling quota exhaustion and potential data exposure
H3	GDPR Art. 5(1)(c), Art. 13; DSA Art. 26	RTB auction broadcasting Art. 9-correlated behavioral context without consent or transparency

Disclosure Timeline & Outcome

Date	Event
2026-06-28	R1 sent to dpo@bitsmedia.com, dpo@muslimpro.com, privacy@muslimpro.com, legal@bitsmedia.com, cc DSB and PDPC Singapore; 3 CRITICAL + 3 HIGH findings; three standing questions posed
2026-07-07 onwards	Six follow-up notices through 2026-09-01, cc extended to EDPS and CERT.at from fourth notice onward; no reply received
2026-09-22	First genuine human reply from ahmadul@bitsmedia.com (Head of Product & Engineering); partial deflection on C1 and C3; four findings unacknowledged; DPO inbox claim made
2026-09-23	RFI-IRFOS R2: DPO inbox claim rebutted; four unaddressed findings explicitly named; all three standing questions repeated verbatim
2026-09-25	RFI-IRFOS R3: on-device verification against v17.9 (versionCode 1709000101); small evidence for BOOT_COMPLETED location access submitted; Tencent IMSDK confirmed; partial Facebook AutolnitEnabled acknowledgment; three questions repeated
2026-09-26	Public embargo closes as stated identically throughout the correspondence; no reply to R3 received
2026-10-17	Report published; four findings remain unaddressed (C2, H1, H2, H3); C1 and C3 disputed but not remediated

Residual Risk & Recommendations

- Remove ByteDance/Pangle and Tencent IMSDK immediately. Any ad network or social feature requiring PRC-jurisdiction SDKs is incompatible with GDPR Art. 9 processing of EU users' religious practice data.
 - Remove all BOOT_COMPLETED receivers that access location, or gate them strictly behind explicit prior consent.
 - Rotate the Firebase API key (muslim-pro-app). Audit Firebase security rules for unauthenticated access. Implement Firebase App Check.
 - Disable Prebid Mobile RTB or replace with contextual-only advertising. Publish a full data-processor list per GDPR Art. 13.
 - Remove AudienceNetworkContentProvider from manifest or gate it behind consent. Do not ship audience_network.dex as a dynamic asset.
 - Establish a DPO contact that is actively monitored and capable of responding to GDPR disclosure notices.
-

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. GDPR Art. 5, 6, 7, 9, 13, 25, 32, 46. DSA Art. 26. PRC National Intelligence Law Art. 7 (2017). REF MP-2026-R1.