Coordinated Security & Privacy Disclosure, Final Report

TikTok for Android (com.zhiliaoapp.musically)

Short-form video platform, one substantive reply in 91 days, a HackerOne redirect

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, ONE REPLY, NEVER A DPO OR LEGAL CONTACT

Target	ByteDance Ltd. (Beijing/Cayman Islands) / TikTok Inc. (Culver City, California, US)
Product audited	TikTok for Android, com.zhiliaoapp.musically, v45.5.4, 129.9MB APK, targetSdk 36
Disclosure reference	REF TIKTOK-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (F1 pre-install attribution / F4 screen capture / F8 China routing, CVSS v4.0 8.7 High)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production TikTok Android application and identified nine findings. The most significant: a plaintext configuration file, extractable from the public APK in under 30 seconds, documenting 58 pre-install attribution partnerships between ByteDance and global carriers and device manufacturers, including Deutsche Telekom, AT&T, T-Mobile, Samsung, and Xiaomi by name, read at first launch before any consent screen is shown to the user.

The application ships 726 internal ByteDance Privacy Engineering Audit certificates verbatim in the public binary, documenting every authorized data collection event including 54 clipboard-read authorizations with no plausible legitimate purpose for the majority of sessions. A 28,940-byte network configuration file is obfuscated with a single-byte XOR key, defeated in under an hour, decoding to 554 domain entries across ByteDance's global infrastructure, including active routing to Volcengine, ByteDance's China-based cloud platform, subject to the PRC Cybersecurity Law, Data Security Law, PIPL, and National Intelligence Law Art. 7, with no EU adequacy decision or Schrems II-compliant transfer mechanism. Active, non-test code implementing screen capture via Android's MediaProjection API exists with no disclosure at the point of capture.

RFI-IRFOS sent ten written notices to security@tiktok.com over 91 days. The only reply, an automated HackerOne redirect two days after the original notice, was declined the same day in writing. No data protection officer, legal, or privacy contact ever engaged with any of the nine findings across the remaining 89 days of the disclosure period.

Scope: Static analysis of the publicly downloaded production TikTok Android APK, on an authorized test device, only. No ByteDance or TikTok backend, account, or infrastructure was accessed or tested. No dynamic runtime tracing of the screen-capture or clipboard-read code paths was performed.

Disposition

R1 sent 20 June 2026 to security@tiktok.com, cc Deutsche Telekom, AT&T, T-Mobile, Samsung, and Xiaomi directly, bcc the Austrian DSB. The only substantive reply in the entire correspondence arrived two days later, on 22 June 2026: an automated redirect to TikTok's HackerOne bug bounty program. RFI-IRFOS declined the same day, in writing, on the basis that a coordinated GDPR disclosure to a controller with EU obligations is not a scope-limited vulnerability bounty submission. Nine further written notices followed through 4 September 2026. None produced a reply, ticket number, or acknowledgment of any kind. No data protection officer, legal, or privacy contact ever engaged.

ID	Severity	Title
F1	CRITICAL	Pre-install attribution network: 58 carrier and OEM partners named verbatim in the public APK
F2	HIGH	726 internal data-collection certificates shipped verbatim in the public APK

ID	Severity	Title
F3	HIGH	XOR-obfuscated network configuration: 554 domains behind a single-byte key
F4	HIGH	Undisclosed MediaProjection screen-capture code, confirmed active by its own audit certificate
F5	MEDIUM	Hardcoded Amazon AWS OAuth2 credential, issued 2018, shipped for approximately eight years
F7	MEDIUM	Over-broad permission set inconsistent with a video-sharing platform's stated purpose
F8	HIGH	Active routing to Volcengine: China-based infrastructure with no EU transfer safeguard
F9	MEDIUM	Transsion device-specific tracking code targeting lower-digital-literacy markets

Subject & Operator Analysis

TikTok is operated by ByteDance Ltd. (headquartered in Beijing, incorporated in the Cayman Islands) through TikTok Inc. (Culver City, California) for the global market outside China. TikTok is an EU-designated Very Large Online Platform under the Digital Services Act, carrying Art. 26 and 27 algorithmic-transparency and Art. 33 systemic-risk-assessment obligations in addition to the GDPR analysis in this report.

Positive Observations

TikTok's in-app permission dialogs are, in RFI-IRFOS's assessment, among the clearer implementations in the industry. The BPEA (ByteDance Privacy Engineering Audit) certification system itself, internal certification of individual data-collection events before they ship, is a more structured privacy-engineering approach than most platforms RFI-IRFOS has audited implement. The problem this report documents is not that the system exists, but that its certificates ship publicly in the APK and that several certified categories, particularly repeated clipboard access, are disproportionate to any stated legitimate purpose.

Findings

F1: Pre-install attribution network: 58 carrier and OEM partners named verbatim in the public APK

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

assets/df_config.json, plaintext and extractable in under 30 seconds, maps 58 df_code integers to named carrier and OEM partners including Deutsche Telekom, AT&T, T-Mobile, Samsung, and Xiaomi, read at first launch before any consent screen is shown.

df_code	Partner	Category
52	Deutsche Telekom	Carrier pre-install
11	AT&T	Carrier pre-install
5/35/36/48	T-Mobile	Multiple carrier campaigns
2/39	Samsung	OEM pre-install
1/29/46/50	Xiaomi	Multiple OEM campaigns
14	preload_kr_girlphone	Gender/age-targeted pre-install

No response was received from TikTok naming this finding. Pre-install attribution creates a tracking record before any consent UI is presented, and the ByteDance-carrier-OEM triangle constitutes undisclosed joint controllership under GDPR Art. 26. Entry 14, preload_kr_girlphone, targets users by gender and likely age, engaging GDPR Recital 38 and COPPA considerations directly. The named carriers and OEMs, cc'd on the original disclosure, received no reply from TikTok either as of publication.

Impact: Users are tracked and attributed to a specific carrier or OEM partnership before they ever see a consent screen, and the carriers and OEMs named in their own device's pre-install configuration were never informed their users would be exposed this way.

Fix: Move partner attribution codes out of the publicly extractable APK, gate all tracking initialization behind the consent screen, and disclose the joint-controller relationship with each named partner under Art. 26.

F2: 726 internal data-collection certificates shipped verbatim in the public APK

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

assets/bpea/collect_cert_fact_detail.json contains 726 ByteDance Privacy Engineering Audit certificates: 54 clipboard-read authorizations, 44 location, 33 contact access, 7 screen capture/MediaProjection, 5 screenshot, 1 IP address via the ByteCast ad network.

No response was received naming this finding. 54 clipboard-read authorizations have no plausible legitimate purpose for the majority of sessions, failing the data minimisation requirement of GDPR Art. 5(1)(c). RFI-IRFOS credits the BPEA system itself as a more structured internal privacy-engineering approach than most platforms implement; the problem is that its certificates ship publicly and that several categories are disproportionate to any stated purpose, not that the certification system exists.

Impact: The scale and specificity of the certified data-collection events, particularly repeated clipboard access, exceeds what a video-sharing platform's core function requires.

Fix: Reduce clipboard-read authorizations to the minimum required for paste-detection features actually exposed to users, and stop shipping the internal certificate manifest in the public APK.

F3: XOR-obfuscated network configuration: 554 domains behind a single-byte key

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 6.9

assets/builtin_network_config, a 28,940-byte binary file, is obfuscated with XOR key 0x55, defeated by frequency analysis in under an hour, decoding to 554 network domain entries across ByteDance's global infrastructure. Three decoded domains match Domain Generation Algorithm patterns and were pending WHOIS verification at time of writing.

No response was received naming this finding. A single-byte XOR provides zero real confidentiality; its only function is to obscure the app's network topology from casual inspection, a transparency failure under DSA Art. 26 and 27 and a failure to disclose processing destinations under GDPR Art. 13(1)(f).

Impact: Independent verification of where TikTok actually routes user data is deliberately obstructed by trivial obfuscation rather than genuine security, impeding the exact kind of audit DSA transparency obligations exist to enable.

Fix: Remove the obfuscation and publish the network configuration, or provide it to regulators and auditors on request; obfuscation that a single evening of static analysis defeats provides no real protection to justify its transparency cost.

F4: Undisclosed MediaProjection screen-capture code, confirmed active by its own audit certificate

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

Obfuscated smali classes in smali_classes23/X/ implement MediaProjectionManager.createScreenCaptureIntent() and MediaProjection.createVirtualDisplay(). This is confirmed as active, non-test code by BPEA certificate bpea-start_screen_capture_intent named in F2. No disclosure of screen recording exists at the point of capture in TikTok's privacy flow.

No response was received naming this finding. RFI-IRFOS did not perform dynamic tracing of this code path and states so explicitly: the finding is that the capability exists, is certified as active in ByteDance's own internal audit system, and carries no user-facing disclosure at the point of use, not that RFI-IRFOS observed a live capture event.

Impact: A confirmed, internally-certified screen-capture capability exists in the shipped binary with no disclosure to the user at the moment it would be used.

Fix: Disclose screen-capture usage explicitly at the point of invocation, and publish the specific feature(s) that rely on this capability.

F5: Hardcoded Amazon AWS OAuth2 credential, issued 2018, shipped for approximately eight years

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:L, 6.9

assets/api_key.txt contains an RSA-SHA256-signed Amazon application OAuth2 JWT, client ID amzn1.application-oa2-client.7834720dfa6a4103bf80f058c534cc61, issued 2018-10-16, extractable by anyone who downloads the app.

No response was received naming this finding. This credential has shipped in every TikTok Android build for approximately eight years.

Impact: A near-decade-old credential remains extractable from every distributed APK, regardless of what current permissions it carries.

Fix: Rotate and properly scope this credential immediately, and add credential-age auditing to the release process.

F7: Over-broad permission set inconsistent with a video-sharing platform's stated purpose

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

REQUEST_INSTALL_PACKAGES (silent APK installation capability), ACCESS_BACKGROUND_LOCATION, SYSTEM_ALERT_WINDOW, and READ_CALL_LOG are all declared in a 342KB AndroidManifest.

No response was received naming this finding. The combination significantly exceeds what a social video platform requires under GDPR Art. 5(1)(c) data minimisation, particularly REQUEST_INSTALL_PACKAGES, which grants a silent app-installation capability with no stated user-facing purpose.

Impact: A permission set including silent APK installation, background location, and call-log access exceeds a video-sharing app's disclosed core function.

Fix: Remove REQUEST_INSTALL_PACKAGES unless tied to a specific, disclosed feature, and scope background location and call-log access to explicit, user-initiated features only.

F8: Active routing to Volcengine: China-based infrastructure with no EU transfer safeguard

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 decoded network configuration (F3) includes active routing to *.volces.com, Volcengine, ByteDance's China-based cloud platform, registered under ICP license 京ICP备15043097号.

No response was received naming this finding. Data routed through Volcengine is subject to the PRC Cybersecurity Law (2017), Data Security Law (2021), PIPL (2021), and National Intelligence Law Art. 7. There is no EU adequacy decision for China, no applicable Art. 49 derogation, and no Schrems II-compliant transfer mechanism visible in the binary that would justify routine commercial routing of EU user data through this infrastructure.

Impact: EU user data is routed to infrastructure subject to Chinese state intelligence-sharing obligations with no demonstrated lawful transfer mechanism.

Fix: Publish the specific Art. 44-49 transfer mechanism covering Volcengine routing, or route EU traffic exclusively through EU-based infrastructure.

F9: Transsion device-specific tracking code targeting lower-digital-literacy markets

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

smali_classes10/BrandTransssionInitTask.smali implements dedicated initialization logic for Transsion devices (TECNO, Infinix, itel), dominant in Sub-Saharan African and South Asian markets, extending the df_config attribution partnership (codes 15/51/57) with device-level code.

No response was received naming this finding. Dedicated device-level integration code, beyond a standard attribution entry, for hardware dominant in markets RFI-IRFOS's own research notes warrant particular scrutiny given lower average digital literacy regarding tracking practices, is a deeper integration than the df_config table alone documents.

Impact: Users of Transsion devices, concentrated in markets with less consumer tracking-literacy infrastructure, receive dedicated device-level tracking integration beyond the standard attribution mechanism applied elsewhere.

Fix: Disclose the Transsion-specific integration's actual scope and purpose separately from the general pre-install attribution disclosure recommended for F1.

Finding	Provision	Concern

Data Protection, Article by Article

Finding	Provision	Concern
F1	GDPR Art. 5(1)(a), Art. 13, Art. 26; DSA Art. 26	Pre-consent tracking, undisclosed joint controllership with 58 named partners
F2	GDPR Art. 5(1)(b)(c), Art. 25; DSA Art. 27	726 certified data-collection events shipped publicly, disproportionate clipboard access
F3	DSA Art. 26, 27; GDPR Art. 13(1)(f)	Trivially-defeated obfuscation of network destinations
F4	GDPR Art. 5(1)(b)	Undisclosed, internally-certified screen-capture capability
F5	OWASP Mobile M9	Near-decade-old hard-coded credential
F7	GDPR Art. 5(1)(c)	Permission set exceeding stated core function
F8	GDPR Art. 44-49	China-routed traffic with no transfer safeguard
F9	GDPR Art. 5	Device-specific tracking concentrated in lower-tracking-literacy markets

Additional Context

The APK contains 38 DEX files, five to twelve times more than comparable applications, with all 27,000-plus non-framework Java classes following a single obfuscated naming pattern. Code minification is standard industry practice; this specific combination, alongside the XOR-obfuscated network configuration (F3) and the 342KB manifest (F7), produces a codebase that is structurally resistant to independent security audit in a way RFI-IRFOS considers inconsistent with the transparency obligations of a Very Large Online Platform under the DSA, without asserting this obfuscation level alone constitutes a scored technical vulnerability.

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to security@tiktok.com, cc Deutsche Telekom/AT&T/T-Mobile/Samsung/Xiaomi, bcc Austrian DSB, nine findings
2026-06-22	Only substantive reply of the entire correspondence: automated redirect to TikTok's HackerOne bug bounty program
2026-06-22 (same day)	RFI-IRFOS declines the routing in writing: a coordinated GDPR disclosure to a controller with EU obligations is not a scope-limited bounty submission
2026-07-23 / 07-27	Follow-ups; three specific questions put on record with a 48-hour response window requested
2026-08-04	48-hour window lapsed six days earlier, treated as Art. 33-relevant
2026-08-12 / 08-15 / 08-24 / 08-31 / 09-04	Continued follow-ups; no DPO, legal, or privacy contact ever found or engaged
2026-09-19	Embargo closes; this report publishes

Ten written notices across 91 days produced exactly one reply, a boilerplate bounty-program redirect two days after the original notice, declined the same day. No data protection officer, legal, or privacy function at ByteDance or TikTok ever engaged with any of the nine findings. None of the carriers or OEMs named and cc'd on the original disclosure, whose own preinstall attribution codes were exposed, replied either.

Residual Risk & Recommendations

- Establish a coordinated-disclosure intake path that reaches a DPO or legal function directly, separate from the HackerOne bug-bounty queue, for disclosures naming GDPR and DSA compliance findings rather than exploitable vulnerabilities.
- Gate all partner-attribution tracking behind the consent screen and disclose the joint-controller relationship with each named carrier and OEM partner.
- Reduce clipboard, location, and screen-capture authorizations to what specific, disclosed features actually require.
- Publish the network configuration rather than obfuscating it, or make it available to regulators and auditors on request.
- Publish the specific Art. 44-49 transfer mechanism covering Volcengine routing, or route EU traffic exclusively through EU infrastructure.
- Rotate the eight-year-old hardcoded AWS credential.
- Disclose the Transsion-specific tracking integration's actual scope to affected users.

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). GDPR Art. 5, 13, 25, 26, 44-49. DSA Art. 26, 27, 33. REF TIKTOK-2026-R1.