Security & Privacy Disclosure, Final Report

Turbo VPN - Safe, Fast Private Proxy for Android (free.vpn.unblock.proxy.turbovpn)

Root level code analysis of a 500M+-install VPN marketed on privacy, with zero reply of any kind across three notices spanning 83 days.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026.

Operator	Innovative Connecting Pte. Limited, 8 Marina View #43-052A Asia Square Tower 1, Singapore 018960 (UEN 201812738K)
Versions Audited	4.3.1.1 / versionCode 2026082111 (23 Aug 2026, original notice)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	4: 1 Critical, 2 High, 1 Medium
Status	NO REPLY OF ANY KIND as of 14 November 2026, 83 days after the original notice, across three separate messages (23 Aug, 12 Sep, 17 Oct 2026).
SHA-256 (base APK)	`39dca01d9c1aa5fae7b664ff7d4fa1557588ba3c48b7e28c06010c44efad0ce7`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 4

4 Architecture & Data Flow 5

5 Engagement Summary 5

6 Findings 6

6.1 C1: Google Mobile Ads SDK initializes via ContentProvider before the app's own GDPR consent screen can render . . . 6

6.2 H1: Nine ad/analytics/attribution SDKs bundled in a tool marketed as privacy-protective, including a Russian-jurisdiction SDK and a PRC ad-mediation SDK with hardcoded mainland-China endpoints . . . 7

6.3 H2: No Art. 27 EU representative named for a Singapore-only legal entity serving EEA/UK users . . . 8

6.4 M1: Full installed-app inventory (QUERY_ALL_PACKAGES) on a device-intermediary app with 500M+ installs . . . 8

7 Impact Analysis 9

8 The Complete Chain 9

9 Data Protection: Article by Article 9

10 Regulatory & Legal Landscape 10

11 Indicators of Compromise & Reproducible Evidence 10

12 Disclosure Timeline & Outcome 11

13 What Turbo VPN Got Right 11

14 Residual Risk & Recommendations 12

Executive Summary

Turbo VPN (free.vpn.unblock.proxy.turbovpn) is operated by Innovative Connecting Pte. Limited, a named Singapore entity (UEN 201812738K) with a named Data Protection Officer (David Lau), installed on 500M+ Android devices. On 23 August 2026 RFI-IRFOS disclosed four findings from a root level code analysis of version 4.3.1.1 under REF TURBOVPN-2026-R1. The operator's corporate identity is not hidden, a genuine and creditable departure from this disclosure wave's usual pattern for free VPN operators, but the binary shows a direct, checkable contradiction between the app's self-marketing ("anonymous and secure internet," "we do not target advertisements based on your personal data") and its actual SDK footprint.

Turbo VPN bundles at least nine independent third-party ad, analytics, and attribution networks, AdMob, Vungle, Unity Ads, InMobi, Bigo Ads, Yandex Mobile Ads, IronSource/LevelPlay, TradPlus, Monetrix, Chartboost, Adjust, AppMetrica, and Zendesk, alongside Firebase, inside a tool whose entire value proposition is that it protects the user's traffic from observation. Two are jurisdictionally notable for a privacy product: Yandex AppMetrica and Yandex Mobile Ads route to Russian-Federation infrastructure, and TradPlus, a PRC-headquartered ad-mediation vendor, ships six hardcoded cn-prefixed API endpoints and a Hong Kong Alibaba Cloud storage bucket compiled directly into the global build distributed to all 500M+ installs, not a China-region-only variant.

Structurally identical to a pattern this programme has documented elsewhere: Google's own Mobile Ads SDK initializes via a ContentProvider (MobileAdsInitProvider, initOrder="100") that Android guarantees runs before any Activity, including the app's own GDPRActivity, whose on-screen text states "we cannot provide our services without your consent" and which forces the app to exit if the user declines. The ad SDK's own initialization plumbing cannot be gated by a consent screen it has not yet been given the chance to render for.

RFI-IRFOS sent the original notice on 23 August 2026, a follow-up on 12 September 2026, and a 35-days-to-publication notice on 17 October 2026. As of 14 November 2026, 83 days after the original notice, no reply of any kind, not even an automated acknowledgment, has arrived from either address contacted.

Scope: Root level code analysis of the Google Play release bundle 4.3.1.1 (base APK SHA-256 above, obtained via APKCombo's mirror of the live Google Play build and cross-checked against the live Play Store listing before analysis): manifest, resources, network security config, and dex-string/grep inventory across all 6 dex files. Passive review of the operator's own public privacy policy, fetched live. No baksmali/smali disassembly was completed this pass (disk-space constrained, not skipped by choice); every finding below is evidenced from the manifest, resources, dex-string content, or native-library inventory, none requires a smali-level control-flow trace to stand. No CallApp, Adobe, or other target's infrastructure, and no Turbo VPN servers, accounts, or API keys, were probed or tested.

ID	Severity	Title
C1	CRITICAL	Google Mobile Ads SDK initializes via ContentProvider before the app's own GDPR consent screen can render
H1	HIGH	Nine ad/analytics/attribution SDKs bundled in a tool marketed as privacy-protective, including a Russian-jurisdiction SDK and a PRC ad-mediation SDK with hardcoded mainland-China endpoints
H2	HIGH	No Art. 27 EU representative named for a Singapore-only legal entity serving EEA/UK users
M1	MEDIUM	Full installed-app inventory (QUERY_ALL_PACKAGES) on a device-intermediary app with 500M+ installs

Finding Status at a Glance

ID	Disclosed	This report	Status as of 14 November 2026
C1	CRITICAL	CRITICAL	No reply of any kind to three notices spanning 83 days; stands exactly as disclosed.
H1	HIGH	HIGH	Same; stands as disclosed.
H2	HIGH	HIGH	Same; stands as disclosed.
M1	MEDIUM	MEDIUM	Same; stands as disclosed.

Subject & Operator Analysis

Innovative Connecting Pte. Limited is a named Singapore private limited company (UEN 201812738K, registered at 8 Marina View #43-052A Asia Square Tower 1, Singapore 018960) with a named Data Protection Officer, David Lau (dataprivacyofficer@inconnecting.com), published in its own privacy policy. This transparency about corporate identity is a genuine positive, uncommon among free VPN operators in this programme's experience, and is credited explicitly in What Turbo VPN Got Right below. It does not extend to engagement: no reply of any kind, not even an automated ticket acknowledgment, has arrived at turbovpn@inconnecting.com or dataprivacyofficer@inconnecting.com across three separate notices (23 August, 12 September, 17 October 2026).

Architecture & Data Flow

Turbo VPN bundles AdMob, Vungle, Unity Ads, InMobi, Bigo Ads, Yandex Mobile Ads, IronSource/LevelPlay, TradPlus, Monetrix, Chartboost, Adjust, AppMetrica, Zendesk, and Firebase, confirmed via manifest-declared activities, providers, and services, not string leftovers. TradPlus ships six cn-prefixed API endpoints (cn-adx-event.tradplusad.com and five others) and a Hong Kong-region Alibaba Cloud OSS storage bucket, compiled into the single global build distributed to all 500M+ installs. Yandex AppMetrica and Yandex Mobile Ads route to yandex.ru, appmetrica.io, and startup.mobile.yandex.net. Google's Mobile Ads SDK initializes via a manifest ContentProvider (MobileAdsInitProvider, initOrder="100"), guaranteed by Android's own component lifecycle to run before any Activity, including the app's own GDPRActivity. On the VPN-specific core question, the native library inventory is StrongSwan/IKEv2, OpenVPN, Shadowsocks/SSR, and Xray only, no cleartext-only protocol library was found, and the network security config restricts cleartext traffic to the loopback interface used for local tunnel plumbing.

Engagement Summary

The original notice went to turbovpn@inconnecting.com and dataprivacyofficer@inconnecting.com on 23 August 2026, with the Austrian DSB and the EDPS in copy. A follow-up restating the findings unchanged went out on 12 September 2026, twenty days later, after no reply or acknowledgment of any kind had arrived. A 35-days-to-publication notice went out on 17 October 2026, fifty-five days without a reply. As of 14 November 2026, eighty-three days after the original notice, no reply of any kind, not an acknowledgment, not an auto-responder, not a single word, has arrived from either address contacted.

Findings

C1: Google Mobile Ads SDK initializes via ContentProvider before the app's own GDPR consent screen can render

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), CVSS scores technical exploitability and gives a pure pre-consent timing defect 0.0

MobileAdsInitProvider (initOrder="100") is declared as a manifest ContentProvider, structurally guaranteed by Android's own component lifecycle to initialize before any Activity in the process, including GDPRActivity, the screen whose own text states "we cannot provide our services without your consent" and which exits the app automatically if the user declines.

```
<provider android:authorities="free.vpn.unblock.proxy.turbovpn.mobileadsinitprovider"
    android:exported="false" android:initOrder="100"
    android:name="com.google.android.gms.ads.MobileAdsInitProvider"/>
<activity android:label="" android:launchMode="singleTop"
    android:name="free.vpn.unblock.proxy.turbovpn.activity.GDPRActivity" .../>

<string name="sure_quit_content">In accordance with user data protection policies, we
    cannot
provide our services without your consent. If you decide to leave this page, the app
    will
exit automatically.</string>
```

For balance: firebase_analytics_collection_enabled, firebase_crashlytics_collection_enabled, and firebase_messaging_auto_init_enabled are all explicitly set to false by default in the manifest, a genuine opt-in posture for Firebase's own telemetry. MobileAdsInitProvider carries no equivalent opt-in gate; its initOrder="100" placement fires unconditionally on every cold start. No reply to this finding has been received across three notices spanning 83 days; it stands exactly as disclosed.

Impact: The Google Mobile Ads SDK begins bootstrap on every one of 500M+ installs' cold starts, including the very first one, before the app's own consent screen, which tells the user the app cannot function without their consent, has had any opportunity to render.

Fix: Open, no reply received across three notices spanning 83 days.

H1: Nine ad/analytics/attribution SDKs bundled in a tool marketed as privacy-protective, including a Russian-jurisdiction SDK and a PRC ad-mediation SDK with hardcoded mainland-China endpoints

---

HIGH, CVSS scoring does not apply to a data-minimization and recipient-disclosure transparency finding; 0.0 (CVSS-B), assessed qualitatively as HIGH given the scale and the product's own privacy marketing

AdMob, Vungle, Unity Ads, InMobi, Bigo Ads, Yandex Mobile Ads, IronSource/LevelPlay, TradPlus, Monetrix, Chartboost, Adjust, AppMetrica, and Zendesk are all confirmed present via manifest-declared components, not string leftovers, alongside Firebase. The operator's own privacy policy names only "Admob, Liftoff, InMobi, Unity and Bigo Ads" as advertising partners; TradPlus, Monetrix, Chartboost, IronSource/LevelPlay, and AppMetrica are compiled into the binary and are not named anywhere in the consumer-facing policy text.

```
cn-adx-event.tradplusad.com   cn-api.tradplusad.com       cn-bidder.tradplusad.com
cn-crosspro-api.tradplusad.com   cn-crosspro-event.tradplusad.com   cn-event.
    tradplusad.com
tp-picture-hk.oss-cn-hongkong.aliyuncs.com
appmetrica.io   startup.mobile.yandex.net   yandex.com   yandex.ru
```

TradPlus is a PRC-headquartered ad-mediation vendor; its six cn-prefixed hostnames and its Hong Kong Alibaba Cloud OSS bucket are compiled into the single global build distributed to every one of the 500M+ installs, not a China-region-only APK variant. Yandex AppMetrica and Yandex Mobile Ads route to Russian-Federation-operated infrastructure. Whether EU-user ad-serving traffic is actually routed to the cn- endpoints specifically, versus western-region ones, is a runtime routing decision this static pass does not resolve and is not asserted here; what is established is that the endpoints and the SDK code capable of calling them are compiled into every copy of the app on Google Play, including copies installed by EEA users. No reply to this finding has been received.

Impact: A user who installs a free VPN specifically to reduce third-party visibility into their online behaviour is, by that same install, handing device- and advertising-ID-linked signals to nine additional companies, two of them headquartered in jurisdictions this programme's own reporting treats as heightened-scrutiny destinations for EU personal data, five of which are not named in the operator's own consumer-facing privacy policy at all.

Fix: Open, no reply received across three notices spanning 83 days.

H2: No Art. 27 EU representative named for a Singapore-only legal entity serving EEA/UK users

HIGH, CVSS scoring does not apply to a representative-designation transparency finding; 0.0 (CVSS-B)

The operator's own privacy policy devotes a dedicated section (7.1) to EEA/UK users and states that GDPR "requires us to outline those practices in a specific manner for users in the EEA and UK," yet nowhere in the roughly 23,000-character policy text is an Art. 27 EU representative named, no address, no dedicated contact, no reference to a representative appointment at all.

```
"...domiciled at 8 Marina View #43-052A Asia Square Tower 1, Singapore 018960. UEN:
    201812738K.
It is therefore governed by and construed in accordance with the laws of the Republic
    of Singapore..."
"7.1 Users in the European Economic Area (EEA)/UK
The EU General Data Protection Regulation (GDPR) of UK GDPR requires us to outline
    those
practices in a specific manner for users in the EEA and UK..."
```

Impact: EEA and UK data subjects and supervisory authorities have no EU-based point of contact for GDPR enforcement purposes on an app the operator's own policy acknowledges serves them; they are directed only to a Singapore address and a general support mailbox.

Fix: Open, no reply received across three notices spanning 83 days.

M1: Full installed-app inventory (QUERY_ALL_PACKAGES) on a device-intermediary app with 500M+ installs

MEDIUM, CVSS scoring does not apply to a data-minimization capability finding; 0.0 (CVSS-B)

QUERY_ALL_PACKAGES and com.android.permission.GET_INSTALLED_APPS are declared, feeding BypassVpnActivity's per-app split-tunneling feature, a legitimate, UI-disclosed capability. It is flagged because a VPN sits between the user and every other app's traffic by design, and the same binary that can see the domain-level shape of all other apps' network traffic also enumerates the full list of every other app installed on the device, alongside the AD_ID and ACCESS_ADSERVICES permission set feeding the nine SDKs in H1.

Impact: The installed-app list is a correlatable, device-fingerprinting-grade signal sitting directly alongside a large, active third-party ad/analytics recipient stack, a capability finding rather than a demonstrated exfiltration.

Fix: Open, no reply received across three notices spanning 83 days.

Impact Analysis

The population affected by C1 is every one of 500M+ installs on every cold start, regardless of jurisdiction. H1's affected population is any EU user of a product marketed specifically on reducing third-party observation of their traffic, who instead has advertising- and device-identifier-linked signals routed to nine companies, two in jurisdictions this programme's reporting treats as heightened scrutiny for EU personal data, five of which are undisclosed in the operator's own consumer-facing policy. H2 leaves every EEA/UK user of this 500M+-install app without a named EU point of contact for GDPR enforcement, despite the operator's own policy acknowledging it serves them.

The Complete Chain

Point of contact: a user installs a free VPN marketed on the promise of reduced third-party observation of their internet activity. Processing: on the very first cold start, before the app's own GDPRActivity, which states the app cannot function without consent, has any chance to render, MobileAdsInitProvider has already begun Google Mobile Ads SDK bootstrap. Expansion: once running, the app's SDK footprint includes eight further ad, analytics and attribution networks beyond Google's, five of which the operator's own privacy policy does not name, including a PRC ad-mediation vendor with six hardcoded mainland-China endpoints and a Russian-Federation analytics vendor, both compiled into the single global build every user, including every EEA user, receives. Enforcement gap: because no Art. 27 EU representative is named despite the policy's own dedicated EEA/UK section, an affected EU user or supervisory authority seeking to act on any of this has no EU-based address to act against. Consequence: a user who chose this specific product to reduce observation of their traffic has instead increased the number of third parties receiving device-linked signals about them, with no EU enforcement contact and, after 83 days and three notices, no engagement of any kind from the operator.

Data Protection: Article by Article

- Art. 7(1): processing (SDK initialization) before consent is obtained (C1).
- Art. 5(1)(a) and Art. 5(2): lawfulness, fairness, and accountability are undermined when the binary cannot implement the sequence the app's own consent screen describes (C1).
- Art. 5(1)(c): data minimization, questioning why a privacy-marketed VPN needs nine independent ad/analytics/attribution networks (H1); and why split-tunneling requires a persistent, full installed-app inventory capability rather than a narrower mechanism (M1).
- Art. 13(1)(e): accurate recipient disclosure; five SDKs compiled into the binary are not named in the operator's own consumer-facing privacy policy (H1).
- Art. 44/46: third-country transfer safeguards for the PRC and Russian-Federation-routed SDKs, a capability finding with the specific transfer trigger unverified from static analysis alone (H1).
- Art. 27(1): a controller not established in the Union and serving EEA/UK data subjects must designate a representative in a Member State; none is named despite the policy's own EEA/UK-specific section (H2).

- Art. 25: data protection by design, for the QUERY_ALL_PACKAGES capability sitting alongside an active third-party data-recipient stack (M1).

Regulatory & Legal Landscape

Innovative Connecting Pte. Limited is domiciled exclusively in Singapore (UEN 201812738K), with no EU establishment named anywhere in the manifest, the Play Store listing's developer contact block, or the privacy policy. Absent an identified EU main establishment and absent any named Art. 27 representative (H2), this Austrian-initiated disclosure routes to the Österreichische Datenschutzbehörde, with the EDPS in copy per standing practice. No NISG or AI Act citation applies to this target; all GDPR article citations above are exact.

Indicators of Compromise & Reproducible Evidence

Artifact	Value
Package	free.vpn.unblock.proxy.turbovpn
Base APK SHA-256 (4.3.1.1)	39dca01d9c1aa5fae7b664ff7d4fa1557588ba3c48b7e28c06010c44efad0ce7
XAPK bundle SHA-256	766ac4f6dd29ae29e7588ff26b72d0acce1511b20709f7f0d9dda9c57cd4f0c4
Firebase API key	AIzaSyAaTaWO39WprhLUxggEbL-UtTZ6uvmVwOk
Firebase project	turbo-vpn-28b76 (firebaseio.com)
TradPlus endpoints (mainland China)	cn-adx-event.tradplusad.com, cn-api.tradplusad.com, cn-bidder.tradplusad.com, cn-crosspro-api.tradplusad.com, cn-crosspro-event.tradplusad.com, cn-event.tradplusad.com
Yandex endpoints (Russian Federation)	yandex.ru, appmetrica.io, startup.mobile.yandex.net
Operator address	Innovative Connecting Pte. Limited, 8 Marina View #43-052A Asia Square Tower 1, Singapore 018960 (UEN 201812738K)

Disclosure Timeline & Outcome

23 August 2026: original notice to turbovpn@inconnecting.com and dataprivacyofficer@inconnecting.com, with the Austrian DSB and EDPS in copy. 12 September 2026: twenty days, no reply or acknowledgment of any kind, RFI-IRFOS restates the findings unchanged. 17 October 2026: 35-days-to-publication notice, fifty-five days without a reply. As of 14 November 2026, eighty-three days after the original notice and across three separate messages, no reply of any kind, not an acknowledgment, not an auto-responder, has arrived from either address contacted.

What Turbo VPN Got Right

- The operator's corporate identity is not hidden: a named legal entity, UEN, and physical address appear in the privacy policy, uncommon among free VPN operators audited in this programme.
- A named, dedicated Data Protection Officer (David Lau, dataprivacyofficer@inconnecting.com) is published, which many targets in this programme lack entirely.
- A real, rendered GDPR consent screen exists at first launch with actual explanatory copy, not a placeholder or a content-free checkbox.
- Firebase Analytics, Crashlytics auto-collection, and Messaging auto-init are all explicitly disabled by default via manifest flags, a genuine opt-in posture for at least this one vendor's telemetry.
- The network security config restricts cleartext traffic to the loopback interface only; no broad cleartextTrafficPermitted="true" base-config was found.
- The native library inventory (StrongSwan/IKEv2, OpenVPN, Shadowsocks/SSR, Xray) shows genuinely encrypted protocol implementations only; no cleartext-only or plaintext-fallback VPN protocol was found.
- A working kill-switch feature exists as real, dedicated code, not only marketing copy.
- No dangerous permissions for call log, SMS, contacts, precise/background location, or microphone recording were found anywhere in the manifest, a comparatively narrow dangerous-permission footprint for this app category.

Residual Risk & Recommendations

Every finding in this report stands exactly as disclosed on 23 August 2026. Three separate notices across 83 days have produced no reply of any kind, not even an automated acknowledgment, the only target in this report's package with zero correspondence of any form. RFI-IRFOS continues weekly APK diffing against the archived 4.3.1.1 build through publication. Whether the VPN session metadata the operator's own policy admits to collecting (connection success, server, country, ISP) extends further than disclosed, and whether the nine ad/analytics SDKs are suppressed for paying subscribers, both remain open questions this static pass could not resolve and are held for a follow-up pass rather than asserted either way.

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 Root level code analysis of the published Google Play release bundle plus the operator's own public legal documents. No Turbo VPN servers, accounts, or API keys were probed or tested. Research conducted under ISO/IEC 29147 and the freedom of scientific research (Art. 17 StGG). REF TURBOVPN-2026-R1.