Coordinated Security & Privacy Disclosure, Final Report

simpliTV for Android (at.simplitv.ott, v4.7.10)

Eight written notices across three addresses that took six weeks to become deliverable, ninety days, one automated ticket acknowledgment, zero substantive replies

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FIVE FINDINGS UNADDRESSED AFTER EIGHT NOTICES

Target	simplitv GmbH / simpli services GmbH & Co KG, Vienna, Austria, with infrastructure and data protection routed through ORS (Oesterreichische Rundfunksender)
Product audited	simpliTV for Android, at.simplitv.ott, v4.7.10 – an ad-free, paid subscription streaming product
Disclosure reference	REF #SIMPLITV-001
R1 sent	2026-06-25
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Facebook codeless event logging on an ad-free paid subscription app, automatically capturing subscriber viewing and purchase behavior for transmission to Meta, 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 25 June 2026, RFI-IRFOS performed static analysis of the production simpliTV Android application, an ad-free paid subscription streaming product, and identified one CRITICAL, three HIGH, and one MEDIUM finding: Facebook codeless event logging (AutoLoggingOnClickListener, ViewOnClickListener, and an in-app purchase billing wrapper) that automatically captures which channels are searched, which content is tapped, navigation used, and subscription purchase behavior, transmitting this to Meta with the actual scope of tracking server-side configurable and not visible in the static binary, a Sentry crash-reporting ContentProvider that initializes at process creation, before any Activity or consent dialog, capturing device IDs, crash traces, app versions, and session data with no consent gate, unlike the app's own correctly-gated OneSignal push implementation, a Firebase API key hardcoded in the production APK, an allowBackup=true configuration with no exclusion rules, meaning login credentials, subscription status, viewing history, and preferences all qualify for Google Cloud backup without specific user consent to that storage, and AD_ID/ADSERVICES_ATTRIBUTION permissions present despite the product carrying no advertising, alongside undocumented PACKAGE_USAGE_STATS and READ_PHONE_STATE permissions.

Every address named in the original notice, datenschutz@simplitv.at, presse@simplitv.at, and presse@ors-group.at, either bounced outright or produced repeated delivery-delay warnings for six weeks; the first message to actually reach a live inbox was sent 12 August to kontakt@simpli.at and datenschutz@ors.at. Across eight written notices over ninety days, the only inbound reply this case ever produced was a single automated customer-service ticket acknowledgment from kontakt@simpli.at. No substantive reply of any kind addressed any of RFI-IRFOS's three standing questions: whether simplitv's data protection team is aware that AutoLoggingOnClickListener transmits paying subscribers' viewing behavior to Meta, whether Meta is named as a recipient in the privacy policy, and whether Sentry's pre-consent initialization has been corrected to match the app's own OneSignal consent gate.

Scope: Static analysis of the publicly downloaded production simpliTV Android APK (v4.7.10), on an authorized test device, only. No simplitv account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 25 June 2026 to datenschutz@simplitv.at, presse@simplitv.at, and presse@ors-group.at, bcc the Austrian Datenschutzbehoerde and CERT.at per the message body. Every one of these addresses either bounced or produced repeated delivery-delay warnings for six weeks; the first message to actually reach a live address was sent 12 August to kontakt@simpli.at and datenschutz@ors.at. Across eight written notices over ninety days, the only inbound reply was a single automated customer-service ticket acknowledgment; no substantive reply of any kind was ever received.

ID	Severity	Title
C1	CRITICAL	Facebook codeless event logging on an ad-free paid subscription app
H1	HIGH	Sentry initializes before any consent gate
H2	HIGH	Firebase API key hardcoded in the production APK
H3	HIGH	allowBackup=true – subscription credentials in Google Cloud backup
M1	MEDIUM	AD_ID/ADSERVICES_ATTRIBUTION and undocumented device permissions in an ad-free app

Subject & Operator Analysis

simplitv GmbH operates the simpliTV streaming product; customer-facing support runs under simpli services GmbH & Co KG, and infrastructure/data-protection matters route through ORS (Oesterreichische Rundfunksender).

Findings

C1: Facebook codeless event logging on an ad-free paid subscription 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

com.facebook.appevents.codeless.CodelessLoggingEventListener/AutoLoggingOnClickListener and com.facebook.appevents.suggestedevents.ViewOnClickListener/ViewObserver, combined with an InAppPurchaseBillingClientWrapper, automatically capture UI interactions, which channels are searched, which content is tapped, navigation used, and subscription purchase behavior, and transmit them to Meta. The actual scope of active tracking is server-side configurable and not visible in the static binary.

simpliTV is an ad-free paid subscription product; this tracking has no advertising purpose the product itself would suggest. No reply of any kind addressed this finding.

Impact: Paying subscribers' detailed viewing and purchase behavior on an explicitly ad-free product may be transmitted to a third-party advertising platform with no matching disclosure.

Fix: Remove or explicitly disclose Facebook codeless event logging, and confirm via server-side configuration audit what data categories are actually transmitted.

H1: Sentry initializes before any consent gate

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

at.simplitv.ott.SentryInitProvider (initOrder=200) and SentryPerformanceProvider (initOrder=100) fire at process creation, before any Activity or consent dialog, capturing device IDs, crash traces, app versions, and session data. The app's own OneSignal push implementation, by contrast, has a correct privacy-consent gate.

No reply of any kind confirmed whether Sentry's initialization has been moved behind a consent gate matching OneSignal's.

Impact: Device and crash-telemetry data is collected before any consent decision is made, inconsistent with the app's own demonstrated capability to gate a comparable SDK correctly.

Fix: Move Sentry initialization behind the same consent gate already implemented for OneSignal.

H2: Firebase API key hardcoded in the production APK

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

Firebase API key AIzaSyBZGUr14kbGMfOC95VLWAd6TjLhgRcAFF4 is extractable from the production APK.

No reply of any kind addressed this finding.

Impact: A production Firebase project's attack surface cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Rotate the exposed key, confirm deny-by-default security rules, and enforce App Check for this project.

H3: allowBackup=true – subscription credentials in Google Cloud backup

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

android:allowBackup=true is declared with no backup_rules.xml exclusions. Login credentials, subscription status, viewing history, and preferences all qualify for Google Cloud backup with no specific user consent to that storage.

No reply of any kind addressed this finding.

Impact: Subscription credentials and viewing history are backed up to a user's personal cloud storage with no comprehensive exclusion policy.

Fix: Define backup_rules.xml excluding login credentials, subscription data, and viewing history.

M1: AD_ID/ADSERVICES_ATTRIBUTION and undocumented device permissions in an ad-free app

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

AD_ID and ADSERVICES_ATTRIBUTION are present despite no advertising in the product. PACKAGE_USAGE_STATS (which apps are running) and READ_PHONE_STATE are declared with no documented purpose.

No reply of any kind addressed this finding.

Impact: Advertising and device-monitoring permissions are held with no apparent purpose consistent with an explicitly ad-free product.

Fix: Remove permissions inconsistent with the product's stated ad-free positioning, or document their actual purpose.

Six Weeks of Dead Addresses, One Automated Acknowledgment

Every address named in the original 25 June notice, datenschutz@simplitv.at, presse@simplitv.at, and presse@ors-group.at, either bounced or produced repeated delivery-delay warnings for six full weeks. The first message to actually reach a live inbox was sent 12 August, over seven weeks after R1, to kontakt@simpli.at and datenschutz@ors.at. The only inbound reply across all eight notices and ninety days was a single automated customer-service ticket acknowledgment; no substantive reply of any kind was ever received.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 13(1)(e), Art. 6(1)	Subscriber viewing/purchase behavior transmitted to Meta with no advertising purpose
H1	GDPR Art. 6/7	Pre-consent crash-telemetry collection
H2	GDPR Art. 32	Hardcoded Firebase key
H3	GDPR Art. 32	Subscription credentials in unrestricted cloud backup
M1	GDPR Art. 5(1)(c)	Advertising and device-monitoring permissions in an ad-free product

Disclosure Timeline & Outcome

Date	Event
2026-06-25	R1 sent to datenschutz@simplitv.at, presse@simplitv.at, presse@ors-group.at; bcc Austrian DSB/CERT.at; 1 CRITICAL + 3 HIGH + 1 MEDIUM findings
2026-06-26 to 2026-07-20	Repeated delivery-delay and failure notices across all three original addresses
2026-08-12	First message reaches a live address (kontakt@simpli.at, datenschutz@ors.at); automated ticket acknowledgment received same day
2026-08-25	Follow-up repeats the three standing questions verbatim, embargo confirmed unchanged
2026-09-06	Follow-up, twenty-five days since the last message, discloses weekly binary re-diffing and an Art. 33(4) staged-reporting notice during the embargo window
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Establish functioning privacy and press contact addresses across all three brand entities involved.
- Remove or explicitly disclose Facebook codeless event logging on this ad-free subscription product.
- Move Sentry initialization behind the same consent gate already implemented for OneSignal.
- Define backup exclusion rules for subscription credentials and viewing history.
- Remove advertising-adjacent permissions inconsistent with an ad-free product’s stated positioning.

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, 7, 13, 32. REF #SIMPLITV-001.