Coordinated Security & Privacy Disclosure, Final Report

Taxefy for Android (at.taxefy.app, v1.0.104, versionCode 20598)

Eight written notices, two legal-threat replies demanding destruction of the analysis, zero technical answers

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FIVE FINDINGS UNADDRESSED, THREE STANDING QUESTIONS NEVER ANSWERED

Target	Taxefy GmbH, Austria
Product audited	Taxefy for Android, at.taxefy.app, v1.0.104 (versionCode 20598)
Disclosure reference	REF AT-TAXEFY-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 a hardcoded Firebase key and Facebook client token enabling forged push notifications to all Taxefy users, CVSS v4.0 8.8, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Taxefy Android application, an Austrian income-tax filing app, and identified two CRITICAL and three HIGH findings: a Firebase API key and a Facebook client token both hardcoded in the shipped APK, present since first release, capable of probing Firebase database rules, reading Remote Config, and forging push notifications to all Taxefy users, an Android Privacy Sandbox configuration setting allowAllToAccess="true" across attribution, custom-audience, and topics categories, granting every third-party SDK in the app, Veriff, Adjust, Facebook, and Sentry, unrestricted access to ad-targeting signals derived from behavior on a tax-filing app, undisclosed in the privacy policy, a Veriff OÜ live biometric video KYC integration (5,063 smali classes, the largest SDK in the APK) performing facial recognition on biometric video without Veriff being named as a processor in the privacy policy or an identifiable explicit Art. 9(2)(a) consent basis, a Facebook Login authentication channel for tax-return sessions sending a signal event to Meta on every login with no identifiable US data-processing agreement in the privacy policy, and an Adjust ad-attribution integration reporting every form-filling and submission action as a conversion event to AppLovin Corporation's US infrastructure, with no mention in the privacy policy.

Taxefy's CEO, Kevin Gruber, replied personally and substantively twice, on 28 and 31 July, but neither reply engaged with the technical findings: the first denied the findings as incorrect, stated no reportable data-security incident existed, invoked copyright and Sec. 5.4 of Taxefy's terms of service against RFI-IRFOS's decompilation of the public APK, and formally demanded, under Sec. 82 UrhG, that all results of that decompilation be destroyed within 14 days and that Taxefy be removed from RFI-IRFOS's website, reserving further legal action. RFI-IRFOS rebutted each claim in writing the same day, citing the Impressum-based accountability of a public company communication, the inapplicability of a company's own terms of service to a non-customer performing external research, and the Software Directive's (2009/24/EC Art. 6) decompilation exception, and declined to destroy the evidence archive. The second reply, on 31 July, reiterated the same demands with an extended deadline, announced Taxefy would cease direct correspondence with RFI-IRFOS's email address, questioned whether RFI-IRFOS's work constituted genuine research rather than a pretext for selling its own paid engagement offerings, and cited RFI-IRFOS's own EU AI Act Art. 50(4) obligations. Neither reply, nor five further written notices over the following seven weeks, ever answered any of RFI-IRFOS's three standing technical questions: when the finding was escalated internally to a data-protection function, the Art. 6/9 legal basis for Veriff biometrics and the Privacy Sandbox grant, and by when the hardcoded Firebase key would be rotated.

Scope: Static analysis of the publicly downloaded production Taxefy Android APK (v1.0.104), via apktool decompilation, on an authorized test device, only. No Taxefy account, backend, or infrastructure was accessed or tested. This decompilation of a publicly distributed binary for the purpose of independent security research is protected under the EU Software Directive (2009/24/EC) Art. 6 decompilation exception and Austria's Forschungsfreiheitsgesetz.

Disposition

R1 sent 21 June 2026 to datenschutz@taxefy.at (bounced, address does not exist) and office@taxefy.at (delivered), bcc the Austrian Datenschutzbehoerde and CERT.at. Taxefy GmbH's CEO, Kevin Gruber, replied twice, on 28 and 31 July, denying the findings without technical rebuttal, invoking copyright and the app's terms of service, and formally demanding destruction of the decompiled analysis within 14 days under Sec. 82 UrhG and removal of Taxefy from RFI-IRFOS's website. RFI-IRFOS rebutted each legal claim in writing both times and declined to destroy the evidence archive. Neither reply, nor any of five further written notices, ever answered the three outstanding technical questions.

ID	Severity	Title
C1	CRITICAL	Firebase API key and Facebook client token hard-coded in the production APK
C2	CRITICAL	Android Privacy Sandbox allowAllToAccess="true" on a tax-declaration app
H1	HIGH	Veriff live biometric video KYC without a disclosed Art. 9(2)(a) legal basis
H2	HIGH	Facebook Login as the authentication channel for tax-return sessions
H3	HIGH	Adjust ad-attribution tracking of tax-filing behavior

Subject & Operator Analysis

Taxefy GmbH is an Austrian company operating the Taxefy income-tax filing app for Android and iOS.

Findings

C1: Firebase API key and Facebook client token hardcoded in the production APK

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N, 8.8

google_api_key AIzaSyALcH6NzBZxXMal5vowyQu7Q7M-z51M4ZE, firebase_database_url https://786635967789.firebaseio.com, and a hardcoded facebook_client_token c15881cf5f3cae4668d7b6763fcb57d1 are present in res/values/strings.xml, present since the app's first release.

Anyone downloading the APK from the Play Store obtains immediate read access to these credentials, sufficient to probe Firebase database rules, read Remote Config, and forge push notifications to all Taxefy users. No technical rebuttal or rotation confirmation was ever provided in either of Taxefy's two replies.

Impact: A tax-filing application's entire user base is exposed to a forged-push-notification phishing vector, in addition to the standard risks a hardcoded Firebase key and OAuth client token carry.

Fix: Rotate both the Firebase key and Facebook client token, restrict the Firebase key to the correct package name and SHA-256 signing fingerprint, and confirm deny-by-default security rules.

C2: Android Privacy Sandbox allowAllToAccess="true" on a tax-declaration 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

res/xml/ad_services_config.xml sets allowAllToAccess="true" for attribution, custom-audiences, and topics categories, combined with ACCESS_ADSERVICES_AD_ID, ATTRIBUTION, CUSTOM_AUDIENCE, and TOPICS permissions and google_analytics_adid_collection_enabled=true. This grants every third-party SDK in the APK, Veriff, Adjust, Facebook, and Sentry, unrestricted access to ad-targeting signals derived from behavior on an Austrian income-tax filing app.

This configuration is not disclosed in the privacy policy. Neither of Taxefy's two replies addressed this finding.

Impact: Behavioral signals from a tax-filing session are made available to every bundled third-party SDK without restriction, with no matching disclosure of that specific configuration.

Fix: Set allowAllToAccess to false for all three Privacy Sandbox categories and restrict access to only the SDKs with a documented, disclosed need.

H1: Veriff live biometric video KYC without a disclosed Art. 9(2)(a) legal basis

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

Veriff OÜ (5,063 smali classes, the largest SDK in the APK) implements FaceDetector, VideoCapture, and FaceDetector$Callback components performing live facial recognition on biometric video. Veriff, an EU processor based in Tallinn, Estonia, is not named as a processor in the privacy policy, and no explicit Art. 9(2)(a) consent basis was identified.

Neither of Taxefy's two replies addressed this finding or the underlying legal-basis question.

Impact: Special-category biometric video data may be processed by a named EU vendor with no disclosed Art. 9(2)(a) consent basis for that specific processing.

Fix: Name Veriff explicitly as a processor in the privacy policy and document the Art. 9(2)(a) legal basis for the biometric verification step.

H2: Facebook Login as the authentication channel for tax-return sessions

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

144 smali classes implement Facebook Login. Meta Platforms (Menlo Park, California, US) receives a signal event on every authentication into a tax-filing session, and the Facebook access-token cache persists tokens between sessions.

No US data-processing agreement was identifiable in the privacy policy. Neither of Taxefy's two replies addressed this finding.

Impact: A login event into a tax-filing session is transmitted to a US technology company with no confirmed Art. 46 transfer mechanism disclosed for that specific processing.

Fix: Disclose Meta Platforms explicitly as a recipient of authentication signal events, with the applicable Art. 46 transfer mechanism, or remove Facebook Login as an authentication option.

H3: Adjust ad-attribution tracking of tax-filing behavior

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

252 smali classes implement Adjust (AppLovin Corp., Palo Alto, California, US). Every user action in the app, filling out the tax form, submitting it, returning to it, is reported to Adjust as a conversion event via AppLovin's US infrastructure.

No mention of Adjust or AppLovin exists in the privacy policy. Neither of Taxefy's two replies addressed this finding.

Impact: Detailed tax-form interaction behavior is transmitted to a US ad-attribution vendor with no matching disclosure or Art. 46 transfer mechanism.

Fix: Disclose Adjust/AppLovin explicitly as a recipient of tax-filing behavioral data, with the applicable Art. 46 transfer mechanism, or remove the integration.

Two Legal-Threat Replies, Zero Technical Answers

Taxefy's CEO, Kevin Gruber, is the only person who ever replied to this disclosure, twice, on 28 and 31 July, and both replies were substantive in tone but adversarial in content. Neither engaged with any of the five technical findings on their merits. The first reply denied the findings, stated no reportable data-security incident existed, invoked copyright and Taxefy's own terms of service against RFI-IRFOS's decompilation of the publicly distributed APK, and formally demanded, under Sec. 82 of the Austrian Copyright Act (UrhG), destruction of all decompilation results within 14 days and removal of Taxefy from RFI-IRFOS's website, reserving further legal action. RFI-IRFOS rebutted each claim in writing the same day: the Impressum-based accountability of a public company communication, the inapplicability of a company's own terms of service to a non-customer performing external research, and the Software Directive's (2009/24/EC) Art. 6 decompilation exception, which permits decompilation for interoperability and security-research purposes independent of a platform's own terms. RFI-IRFOS declined to destroy the evidence archive. The second reply, three days later, reiterated the same demands with an extended deadline, announced Taxefy would cease direct correspondence with RFI-IRFOS's email address, and questioned whether RFI-IRFOS's activity constituted genuine research rather than a pretext to sell paid engagement offerings. RFI-IRFOS rebutted this as well and restated the three outstanding technical questions, which, across both replies and five further written notices over the following seven weeks, were never answered.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Hardcoded Firebase key and Facebook token enabling forged push
C2	GDPR Art. 5(1)(c), Art. 6(1), Art. 13(1)(e)	Unrestricted Privacy Sandbox access for every bundled SDK
H1	GDPR Art. 9(1)/(2)(a), Art. 13(1)(e)	Undisclosed biometric video processor, no consent basis identified
H2	GDPR Art. 6(1), Art. 13(1)(e), Art. 46	Undisclosed authentication-signal transfer to a US recipient
H3	GDPR Art. 6(1), Art. 13(1)(e), Art. 46	Undisclosed tax-behavior tracking transferred to US infrastructure

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@taxefy.at (bounced) and office@taxefy.at (delivered), bcc Austrian DSB/CERT.at; 2 CRITICAL + 3 HIGH findings
2026-07-28	Kevin Gruber replies, denying findings and demanding destruction of the decompiled evidence under Sec. 82 UrhG; RFI-IRFOS rebuts the same day
2026-07-31	Gruber replies again, reiterating demands, announcing correspondence will cease, questioning RFI-IRFOS's research legitimacy; RFI-IRFOS rebuts again
2026-08-15	Follow-up notes Taxefy's own 11 August deadline passed four days earlier with no reply
2026-09-03	Follow-up names the pattern 'Decompile-Destruction-Pivot,' sets a final 48-hour deadline, discloses weekly SHA-256 re-hashing during the embargo, reaffirms 19 September unchanged
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes; no reply since 3 September

Residual Risk & Recommendations

- Answer the three outstanding technical questions directly, separate from the copyright and terms-of-service arguments already rebutted.
- Rotate the exposed Firebase key and Facebook client token.
- Set allowAllToAccess to false across all three Privacy Sandbox categories.
- Name Veriff explicitly as a biometric-data processor with a documented Art. 9(2)(a) legal basis.
- Disclose Facebook Login and Adjust/AppLovin as recipients with applicable Art. 46 transfer mechanisms, or remove the integrations.

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, 9, 13, 32, 46. Decompilation protected under EU Software Directive (2009/24/EC) Art. 6 and Austria's Forschungsfreiheitsgesetz. REF AT-TAXEFY-2026-R1.