Coordinated Security & Privacy Disclosure, Final Report

Grokio for Android (com.grokiolabs.Grokio, v6.1.5, build 773) – a single APK serving six branded communities: Grokio, Grommr, Feabie, PupSpace, Ferzu, and Chasable

Five written notices, ninety-one days, two identical automated ticket acknowledgments, zero human replies

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

Target	Grokio Communities LLC (production Sentry organization registered as 'sky-apps-inc', a discrepancy from the self-disclosed operating entity, never resolved)
Product audited	Grokio for Android, com.grokiolabs.Grokio, v6.1.5 build 773, a single APK serving six branded communities
Disclosure reference	REF GROKIO-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 undisclosed shared data infrastructure across six adult communities processing Art. 9 special-category data, 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 20 June 2026, RFI-IRFOS performed static analysis of the production Grokio Android application and identified three CRITICAL and four further findings, three HIGH and one MEDIUM: a single APK serving six distinct adult community brands, Grokio, Grommr, Feabie, PupSpace, Ferzu, and Chasable, all sharing one Firebase project, one CCBill billing account, one Sentry organization, and one Expo EAS project, meaning a Feabie user's feedism-community profile data and a Grommr user's gay-identity data co-reside in the same backend with no disclosed shared-infrastructure relationship, a Firebase API key hardcoded in the production APK enabling FCM probing and auth enumeration against all six communities' user bases, an absent Network Security Configuration leaving all API traffic across six adult/kink platforms, including sexual profiles, private messages, location data, and payment sessions, without certificate pinning, a background-location permission whose continuous collection is not justified by the app's stated 'see who's nearby' purpose given the intimate behavioral patterns it can reveal across gay, BDSM, and feedism communities, a profile field processing disease/health-status information constituting Art. 9 special-category data, thirteen internal Atlassian Jira Service Desk URLs hardcoded in the production bundle aiding potential social engineering against the support team, and an Expo EAS project ID and Sentry organization name ('sky-apps-inc') inconsistent with the self-disclosed operating entity, raising an Art. 13 controller-identity disclosure question.

Across five written notices over ninety-one days, cc'd or bcc'd to the Austrian Datenschutzbehoerde and CERT.at, the only inbound correspondence was two identical automated Jira Service Desk ticket acknowledgments. No substantive human reply was ever received. None of RFI-IRFOS's standing questions, on whether users of each community are individually informed under Art. 13(1)(e) that their special-category data shares infrastructure with five other communities, whether a DPIA under Art. 35 covers this shared architecture, or whether the lead supervisory authority was notified under Art. 33, ever received an answer.

Scope: Static analysis of the publicly downloaded production Grokio Android APK (v6.1.5, build 773), on an authorized test device, only. No Grokio account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to support@grokiolabs.com, bcc the Austrian Datenschutzbehoerde and CERT.at, with the Austrian DSB moved to visible cc from 23 July onward. Across five written notices over ninety-one days, the only inbound correspondence was two identical automated Jira Service Desk ticket acknowledgments; no substantive human reply was ever received.

ID	Severity	Title
C1	CRITICAL	One APK, six adult communities – undisclosed shared data infrastructure
C2	CRITICAL	Firebase API key hardcoded in the production APK
C3	CRITICAL	No Network Security Configuration – no certificate pinning

ID	Severity	Title
H1	HIGH	Background location permission on sexual/kink platforms
H2	HIGH	Disease/health profile field – Art. 9 health data processing
H3	HIGH	Internal Atlassian Jira service desk URLs hardcoded in the production bundle
M1	MEDIUM	EAS project ID and Sentry organization inconsistent with the self-disclosed operating entity

Subject & Operator Analysis

Grokio Communities LLC self-discloses as the operating company behind each of its six community brands. The production Sentry organization is registered under a different name, sky-apps-inc, a discrepancy RFI-IRFOS flagged as an Art. 13 controller-identity concern that was never resolved by the target.

Findings

C1: One APK, six adult communities – undisclosed shared data infrastructure

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 package com.grokiolabs.Grokio contains activity aliases for Grokio, Grommr, Feabie, PupSpace, Ferzu, and Chasable, all served by a single Firebase project (api-project-505297410678), one CCBill billing account, one Sentry organization (sky-apps-inc), and one Expo EAS project. A Feabie user's feedism-community profile data and a Grommr user's gay-identity data co-reside in the same Firebase backend.

No reply of any kind addressed whether users of each community are individually informed that their special-category data shares infrastructure with the other five communities.

Impact: Special-category data revealing sexual orientation and sexual practices across six distinct communities shares a single backend with no disclosed relationship between them, concentrating risk and cross-community exposure in one infrastructure failure.

Fix: Disclose the shared-infrastructure relationship to users of each community individually, and document the Art. 26/28 governance covering it, or isolate each community's data.

C2: 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

google_api_key AIzaSyAj_LtB5z5lWE8afVGMrJTszCTtXrOTCuA, gcm_defaultSenderId 505297410678, google_app_id 1:505297410678:android:ea3d04cc962d566e, and firebase_database_url https://api-project-505297410678.firebaseio.com are hardcoded in res/values/strings.xml. Realtime Database returned 'Permission denied' for unauthenticated reads at test time, but the exposed key still enables FCM probing and auth enumeration against all six communities' user bases.

No reply of any kind addressed this finding.

Impact: Authentication enumeration and push-messaging probing remain possible against all six communities' user bases via the exposed key, independent of the database's own access rules.

Fix: Rotate the exposed key, restrict it to the correct package name and SHA-256 signing fingerprint, and confirm Firebase Auth rate-limiting is in place.

C3: No Network Security Configuration – no certificate pinning

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

No network_security_config.xml exists anywhere in the APK. All API traffic for all six adult/kink platforms, sexual profiles, private messages, location data, and payment sessions, has no certificate pinning.

No reply of any kind addressed this finding.

Impact: Traffic carrying sexual profile, private message, location, and payment data across six platforms is susceptible to interception by any attacker able to install a trusted certificate authority on the user's device or network.

Fix: Implement certificate pinning for all six communities' API traffic.

H1: Background location permission on sexual/kink platforms

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 manifest declares both ACCESS_FINE_LOCATION and ACCESS_BACKGROUND_LOCATION. In the context of gay, BDSM, and feedism communities, background location continuously reveals intimate behavioral patterns, partner locations, venues, LGBTQ+ spaces, and clinics.

The stated purpose, 'see who's nearby,' does not justify background collection when the app is not in active use. No reply of any kind addressed this finding.

Impact: Continuous background location collection on communities organized around sexual orientation and sexual practice can reveal intimate behavioral patterns well beyond the stated proximity feature.

Fix: Restrict location collection to foreground use only, consistent with the stated 'see who's nearby' purpose.

H2: Disease/health profile field – Art. 9 health data processing

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 bundle contains the profile field string 'Aroma/Olor corporal_disease' and STI-adjacent string references in form contexts. Processing of disease or health status constitutes GDPR Art. 9(1) health data.

Explicit consent layering specific to this data category was not evident from static analysis. No reply of any kind addressed this finding.

Impact: Health-status data may be processed under the same general profile-completion consent as non-sensitive fields, rather than the explicit Art. 9(2)(a) consent that category requires.

Fix: Implement a distinct, explicit consent flow specific to disease/health-status profile fields.

H3: Internal Atlassian Jira service desk URLs hardcoded in the production bundle

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 least thirteen internal Atlassian Jira Service Desk URLs are embedded in the production JS bundle, including issue-type IDs and help-article identifiers, exposing internal project structure and support-ticket categories across all six platforms.

No reply of any kind addressed this finding.

Impact: Exposed internal ticketing structure aids social-engineering and phishing attempts against the support team.

Fix: Strip internal Jira Service Desk URLs and issue-type identifiers from the production bundle.

M1: EAS project ID and Sentry organization inconsistent with the self-disclosed operating entity

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

The production bundle contains Expo EAS Project ID fd13fe19-0aaa-4f50-bfc4-294ed4f5dc2a and Sentry organization 'sky-apps-inc,' inconsistent with the disclosed operating entity, Grokio Communities LLC.

This discrepancy is relevant to GDPR Art. 13 disclosure requirements regarding the identity of the actual data controller and was never resolved by the target.

Impact: Users cannot independently confirm which legal entity actually operates the infrastructure processing their special-category data.

Fix: Reconcile and publish the actual controlling entity name consistent with infrastructure ownership records.

Five Notices, Two Ticket Numbers, Zero Humans

Across five written notices and ninety-one days, the only inbound correspondence in this case was two identical automated Jira Service Desk ticket acknowledgments (SVC-330262, SVC-331835). RFI-IRFOS's own follow-ups state this explicitly in-band: 'twenty-six days, two automated Jira ticket acknowledgments, zero humans' and 'seventy-eight days, two ticket numbers, zero humans.' No substantive human reply was ever received.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 9(1), Art. 13(1)(e), Art. 26	Undisclosed shared infrastructure across six special-category-data communities
C2	GDPR Art. 32	Hardcoded Firebase key enabling auth enumeration across all six communities
C3	GDPR Art. 32(1)(a)	No certificate pinning on sexual profile, message, location, and payment traffic
H1	GDPR Art. 5(1)(c), Art. 9	Background location collection beyond the stated proximity purpose
H2	GDPR Art. 9(2)(a)	Health/disease-status data without a distinct consent flow
H3	GDPR Art. 32	Internal ticketing infrastructure exposed in the production bundle
M1	GDPR Art. 13	Controller-identity inconsistency between disclosed entity and infrastructure records

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to support@grokiolabs.com , bcc Austrian DSB and CERT.at; 3 CRITICAL + 4 further findings; automated Jira ack (SVC-330262) same day
2026-06-28	Follow-up #1, eight days, no reply, response deadline set 2 July; automated Jira ack (SVC-331835)
2026-07-23	Follow-up #2, twenty-six days, Austrian DSB moved to visible cc, staged Art. 33(4) notification option noted as available
2026-08-25	Follow-up #3, sixty-six days, states weekly SHA-256 re-diffing of the APK during the embargo period
2026-09-06	Follow-up #4, seventy-eight days, full chronology restated, new response deadline of 12 September set
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Disclose the shared-infrastructure relationship across all six communities to each community's users individually.
- Conduct and publish an Art. 35 DPIA covering the shared-infrastructure architecture across special-category-data communities.
- Implement certificate pinning across all six communities' API traffic.
- Restrict location collection to foreground use only.
- Reconcile the controller-identity inconsistency between the disclosed operating entity and infrastructure ownership records.

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, 9, 13, 26, 32, 33, 35. REF GROKIO-2026-R1.