Coordinated Security & Privacy Disclosure, Final Report

Fet (de.ideawise.fet)

BDSM and kink community platform, three simultaneous GDPR Art. 9 special categories

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, SIX AUTOMATED REPLIES, ZERO SUBSTANTIVE RESPONSE

Target	ideawise GmbH, Germany
Product audited	Fet for Android, de.ideawise.fet, v14.3.0, build 106
Disclosure reference	REF FET-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (F1 Agora / F4 Mintegral, CVSS v4.0 8.7 High) / F2, F3 transport security score 8.6 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 Fet Android application and identified nine findings, five CRITICAL, four HIGH. Fet processes at minimum three simultaneous GDPR Art. 9 special categories in the same user profile: sexual practices, BDSM identity, and racial or ethnic origin, a combination not seen elsewhere in RFI-IRFOS's dating and community-app research series, and the technical safeguards protecting that data are among the weakest RFI-IRFOS has documented.

Live BDSM video and audio sessions are routed through the Agora RTC SDK, a Chinese company subject to China's Cybersecurity Law and PIPL; independent research (Citizen Lab, 2021) has documented Agora routing streams through mainland China servers regardless of user location. Separately, the application ships with no network_security_config.xml at all, not even the system-CA baseline other audited dating apps declared, meaning every category of traffic, live video, private intimate media in the app's own 'Secret Gallery' feature, and profile data including BDSM roles and ethnicity, is transmitted with zero certificate pinning. For a BDSM community where identity exposure carries real-world safety consequences beyond the ordinary privacy harm, this is not an abstract finding.

RFI-IRFOS's original notice bounced against a misconfigured mail server; once redirected to the correct domain, every subsequent send produced an automated acknowledgment, six in total, but never a substantive human reply across 91 days. All nine findings stand exactly as originally reported.

Scope: Static analysis of the publicly downloaded production Fet Android APK, on an authorized test device, only. No ideawise GmbH backend, account, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026; both originally-published addresses, privacy@fet.app and support@fet.app, bounced immediately with a misconfigured-server error. RFI-IRFOS located and resent to the corrected domain, support@fet-app.com, receiving automated Zendesk acknowledgments in return on every subsequent send, six in total, but no substantive human reply across 91 days and multiple follow-ups.

ID	Severity	Title
F1	CRITICAL	Agora RTC: live BDSM video and audio sessions routed through Chinese infrastructure
F2	CRITICAL	Secret Gallery: intimate media sharing with zero certificate pinning
F3	CRITICAL	No network_security_config.xml anywhere in the application: zero TLS hardening
F4	CRITICAL	Mintegral/Mbridge: a documented fraudulent Chinese ad network on an Art. 9 sexual-practice platform
F5	CRITICAL	Firebase API key hardcoded in production APK

ID	Severity	Title
F6	HIGH	ACCESS_ADSERVICES_TOPICS: the most severe Topics API finding in this research series

Subject & Operator Analysis

ideawise GmbH (Germany) operates Fet, a BDSM and kink community platform. The German Federal Commissioner for Data Protection and Freedom of Information (BfDI) is the relevant federal authority for a German-registered developer and was bcc'd throughout this correspondence, alongside the Austrian DSB and CERT.at.

Findings

F1: Agora RTC: live BDSM video and audio sessions routed through Chinese 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

io.agora.rtc2 (AgoraRtcEngine, AgoralidVideoDeviceManager) provides Fet's live video and audio features. Agora is a Chinese company subject to China's Cybersecurity Law and PIPL; Citizen Lab documented in 2021 that Agora routes streams through mainland China servers regardless of user location.

No response was received naming this finding. Live video of sexual practices, voice audio of intimate sessions, and biometric video data of EU users, all GDPR Art. 9(1) special category data, pass through Chinese infrastructure under PIPL jurisdiction with no EU adequacy decision for China.

Impact: Live intimate video and audio sessions on a BDSM platform are routed through infrastructure subject to Chinese state access laws, with no EU transfer safeguard.

Fix: Replace Agora with an EU-compliant RTC provider or implement and publish a verified Art. 44-49 transfer mechanism.

F2: Secret Gallery: intimate media sharing with zero 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

Fet's 'Secret Gallery' feature lets users share private intimate photos and videos under 30-minute or permanent access grants (GRANT_ACCESS_SECRET_GALLERY_FOREVER, REQUEST_ACCESS_SECRET_GALLERY). No network_security_config.xml exists anywhere in the APK.

No response was received naming this finding. Upload and download of intimate BDSM media through this specific feature is transmitted with no certificate pinning, susceptible to MITM interception on any compromised network.

Impact: Private intimate media shared through Fet's own dedicated privacy feature is exposed to interception with no client-side transport defense.

Fix: Implement certificate pinning specifically for all Secret Gallery upload and download traffic as a priority ahead of general app-wide pinning.

F3: No network_security_config.xml anywhere in the application: zero TLS hardening

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 NSC file exists in the APK at all, not even a system-CA-only baseline. All traffic, live BDSM video, Secret Gallery media, profile data including BDSM roles and ethnicity, and private messages, is unprotected.

No response was received naming this finding. This is structurally worse than every other dating app in RFI-IRFOS's research series: Tinder and Hinge at least declared a system-CA base configuration. Fet has none. For a community where identity exposure carries real-world safety risk beyond the ordinary privacy harm, this is not an abstract vulnerability.

Impact: Every category of Fet's traffic, without exception, is susceptible to MITM interception by any system-trusted CA on a compromised network.

Fix: Implement certificate pinning application-wide as the single highest-priority remediation in this report.

F4: Mintegral/Mbridge: a documented fraudulent Chinese ad network on an Art. 9 sexual-practice platform

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.mbridge, a Chinese ad network documented in 2020 for unauthorized device-data exfiltration and click-injection fraud, is integrated in Fet. This is the third occurrence of Mintegral in RFI-IRFOS's research series, also found in Lovoo and Grokio.

No response was received naming this finding. Any behavioral data Mintegral exfiltrates from a BDSM platform constitutes Art. 9 sexual-practice data transmitted to China with no adequacy framework.

Impact: Sexual-practice behavioral signals are exposed to an ad network with a documented history of unauthorized collection, transmitted to Chinese infrastructure with no transfer safeguard.

Fix: Remove Mintegral or implement a verified Art. 44-49 transfer mechanism and obtain specific Art. 9(2) consent.

F5: Firebase API key hardcoded in production APK

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

AIzaSyAgZOwVDBG1QeyY6awhXIKXd9ckQ5oHksc, project fet-app, database fet-app.firebaseio.com. The database returns 'Permission denied' for unauthenticated access, but the credential remains shipped.

No response was received naming this finding. The key enables FCM token enumeration against all registered Fet users, a community with heightened sensitivity to unwanted contact given the nature of the platform.

Impact: FCM token enumeration is possible against a user base for whom unwanted contact carries elevated real-world risk.

Fix: Rotate the key, restrict it to the production certificate fingerprint, and enable Firebase App Check.

F6: ACCESS_ADSERVICES_TOPICS: the most severe Topics API finding in this research series

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 manifest declares android.permission.ACCESS_ADSERVICES_TOPICS. The Android Topics API infers interest categories from app usage and shares them with advertising partners.

No response was received naming this finding. Explicit BDSM and fetish behavioral signals enter Google's commercial advertising Topics graph with no Art. 9(2) legal basis, the most severe instance of this specific finding across RFI-IRFOS's full research series given the specificity of the inferred category.

Impact: BDSM and fetish behavioral interest signals enter Google's commercial advertising infrastructure with no special-category legal basis.

Fix: Disable Topics API participation entirely for this application category, or obtain explicit Art. 9(2)(a) consent specific to this data flow.

Impact Analysis

Fet's own profile schema, sexual practices, BDSM role and kink identity, and racial or ethnic origin (the field Appartenance ethnique, confirmed in the app bundle), combines three distinct GDPR Art. 9 special categories in a single user record, a combination RFI-IRFOS has not documented elsewhere in its research series. Each category independently requires explicit Art. 9(2)(a) consent; their combination, on a platform with no certificate pinning at all and a live-video pipeline routed through Chinese infrastructure, produces a risk profile distinct from an ordinary dating app. For a BDSM community specifically, exposure of identity, kink preferences, or intimate media is not merely a privacy harm in the abstract sense this report uses elsewhere; it carries real-world social and safety consequences for the individuals affected, a distinction worth stating plainly rather than leaving implicit in the article citations alone.

Data Protection, Article by Article

Finding	Provision	Concern
F1	GDPR Art. 9(1), Art. 5(1)(f), Art. 44-49	Live intimate video/audio routed through Chinese infrastructure
F2, F3	GDPR Art. 32(1)(a)	Zero certificate pinning anywhere, including the app's own dedicated privacy feature
F4	GDPR Art. 5(1)(a), Art. 44-49	Sexual-practice data exposed to a documented fraudulent ad network
F5	GDPR Art. 32	Exposed backend credential on a community with heightened contact-safety sensitivity
F6	GDPR Art. 9(1), Art. 5(1)(c)	BDSM/fetish signals entering commercial ad-targeting infrastructure

Additional Findings

- F7: the profile field Appartenance ethnique (ethnic background) confirms explicit Art. 9(1) racial/ethnic origin collection, the third simultaneous special category alongside sexual practice and BDSM identity data.
- F8: the Meta SDK creates a pipeline of BDSM behavioral signals to Meta's advertising infrastructure, crossable with a real-identity Facebook account on the same device (GDPR Art. 9(1), Art. 26).
- F9: eight simultaneous ad networks (Mintegral, AppLovin, IronSource, InMobi, Digital Turbine/FyBer, MoLoco, Unity Ads, Verve) receive behavioral signals from an Art. 9 sexual-practice platform with no documented legal basis.

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to privacy@fet.app and support@fet.app; both bounce immediately, misconfigured remote server
2026-06-20 (same day)	Corrected address located and resent to support@fet-app.com
2026-08-15	Resend confirmed via automated Zendesk acknowledgment, 56 days silent otherwise
2026-08-25	66-day follow-up, automated Zendesk acknowledgment received same day, no human reply
2026-09-04	76-day follow-up, automated Zendesk acknowledgment received same day, no human reply
2026-09-19	Embargo closes; this report publishes

Six automated Zendesk acknowledgments across the correspondence, never a substantive human reply. All nine findings, three simultaneous Art. 9 special categories among them, stand exactly as originally reported.

Residual Risk & Recommendations

- Implement certificate pinning application-wide immediately; this is the single highest-priority item given the complete absence of any existing TLS hardening.
- Replace Agora with an EU-compliant RTC provider or implement a verified Art. 44-49 mechanism for live video/audio.
- Remove Mintegral or implement a verified transfer mechanism and specific Art. 9(2) consent.
- Disable Topics API participation or obtain explicit consent specific to BDSM/fetish behavioral signals.
- Layer separate, explicit Art. 9(2)(a) consent for each of the three special categories collected: sexual practice, BDSM identity, and ethnic origin.
- Rotate the exposed Firebase credential.

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, 9, 26, 32, 44-49. REF FET-2026-R1.