Coordinated Security & Privacy Disclosure, Final Report

Lovoo (net.lovoo.android)

Dating platform, ParshipMeet Group, largest DACH-market dating app in this research series

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

Target	ParshipMeet Holding GmbH, Speersort 10, 20095 Hamburg, Germany
Product audited	Lovoo for Android, net.lovoo.android, v228.2, build 22802, 188MB APK
Disclosure reference	REF LOVOO-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 Mintegral / C3 FaceUnity, CVSS v4.0 8.7 High) / C4 broken cert pinning scores 8.6 High

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Findings 4

3.1 C1: Chucker HTTP debug interceptor shipped active in the production APK: a live, ongoing exposure 5

3.2 C2: Mintegral/Mbridge SDK: a documented fraudulent Chinese ad network on a sexual-orientation data platform 5

3.3 C3: FaceUnity biometric SDK: facial data to Chinese infrastructure, no adequacy decision 6

3.4 C4: Broken network_security_config.xml: a literal syntax error disables certificate pinning for the API gateway 6

3.5 H5: Development Firebase URL and API key hardcoded in the production APK 7

3.6 H6: Seven simultaneous ad networks on a sexual-orientation data platform . . 7

3.7 H7: Braze marketing automation triggered on Art. 9 behavioral data 8

4 Data Protection, Article by Article 8

5 Additional Findings 9

6 Disclosure Timeline & Outcome 9

7 Residual Risk & Recommendations 10

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Lovoo Android application and identified nine findings, four CRITICAL, four HIGH, one MEDIUM. Of every dating app RFI-IRFOS has audited in this research series, Lovoo presents the most severe technical security posture, headlined by a debugging tool shipped active in the production build.

The Chucker HTTP debug interceptor, a library whose own documentation explicitly prohibits production use, is fully initialized in the shipped APK and actively logging every API request and response, including authentication tokens, private messages, and profile fields such as sexual orientation, to a local database on every installed copy of the app. This is not a theoretical exposure from static analysis; it is a live, ongoing one on every device running the app today. Separately, a literal syntax error in the network security configuration, a stray pair of quotation marks around a domain name, silently disables certificate pinning for the entire API gateway, and two Chinese SDKs, one with a documented history of unauthorized data collection and click-injection fraud, the other processing facial biometric data, transmit user data to Chinese infrastructure with no EU adequacy mechanism.

RFI-IRFOS sent five written notices over 91 days. The only response of any kind was a single automated Zendesk ticket confirmation on 28 June 2026. No human at ParshipMeet Group, the operator of Lovoo, ever engaged on this specific case, in contrast to the sibling Parship case published the same day, where named ParshipMeet Group staff did engage, disputed the findings, and were answered in turn. All nine findings here stand unconfirmed, undisputed, and unaddressed.

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

Disposition

R1 sent 20 June 2026 to privacy@lovoo.com (security@lovoo.com bounced immediately), bcc the Hamburgische Beauftragte fuer Datenschutz und Informationsfreiheit and the Austrian DSB. Five written notices followed: an R2 escalation on 28 June naming a live GDPR Art. 33 breach-notification deadline, an R3 with a final deadline on 3 July, and further follow-ups on 24 July and 4 September 2026. The only response of any kind across the entire correspondence is a single automated Zendesk ticket confirmation on 28 June. Lovoo is a sibling ParshipMeet Group brand to Parship, published separately by RFI-IRFOS the same day; unlike Parship, no named human at ParshipMeet Group ever engaged on this specific case.

ID	Severity	Title
C1	CRITICAL	Chucker HTTP debug interceptor shipped active in the production APK: a live, ongoing exposure
C2	CRITICAL	Mintegral/Mbridge SDK: a documented fraudulent Chinese ad network on a sexual-orientation data platform

ID	Severity	Title
C3	CRITICAL	FaceUnity biometric SDK: facial data to Chinese infrastructure, no adequacy decision
C4	CRITICAL	Broken network_security_config.xml: a literal syntax error disables certificate pinning for the API gateway
H5	HIGH	Development Firebase URL and API key hardcoded in the production APK
H6	HIGH	Seven simultaneous ad networks on a sexual-orientation data platform
H7	HIGH	Braze marketing automation triggered on Art. 9 behavioral data

Subject & Operator Analysis

ParshipMeet Holding GmbH (Hamburg, Germany) operates Lovoo alongside Parship, both audited by RFI-IRFOS on 20 June 2026. The Hamburgische Beauftragte fuer Datenschutz und Informationsfreiheit (HmbBfDI) is the competent supervisory authority as ParshipMeet Group's home jurisdiction and was bcc'd throughout. Where the Parship case, published the same day as this report, saw sustained engagement from named ParshipMeet Group staff who disputed the findings, this Lovoo case saw none: the only response of any kind across five written notices and 91 days was a single automated Zendesk ticket confirmation.

Findings

C1: Chucker HTTP debug interceptor shipped active in the production APK: a live, ongoing exposure

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

com.chuckerteam.chucker (262 classes), a development-only HTTP traffic inspector whose own documentation explicitly prohibits production use, is fully initialized in Lovoo's OkHttp call chain via ChuckerInterceptor and ChuckerCollector, logging all API requests and responses.

No response was received naming this finding. Every auth token, session cookie, private message, and profile field, including sexual orientation, location, and photos, is logged in plain text to a local SQLite database on the user's device. Any app holding BIND_NOTIFICATION_LISTENER_SERVICE can silently read this data via Chucker's own notification; on rooted devices the database is trivially accessible. This is a live data exposure under GDPR Art. 4(12) on every installed copy of the app, not a latent misconfiguration, which is why RFI-IRFOS's second notice treated it as a formal Art. 33 escalation rather than a routine follow-up. The CVSS vector reflects that reading this data requires local device access (AV:L), the same reason its Base score sits lower than the qualitative CRITICAL label; the report keeps that label because of the finding's live, already-occurring nature rather than its remote reach.

Impact: Every user's authentication tokens, private messages, and Art. 9 profile fields are logged in plain text on-device, readable by any co-located app with notification-listener access or anyone with physical or root access to the device.

Fix: Remove Chucker from the production build immediately and confirm via a fresh binary pull that it no longer initializes in any release configuration.

C2: Mintegral/Mbridge SDK: a documented fraudulent Chinese ad network on a sexual-orientation data 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 (3,960 smali classes, the largest single SDK in the APK). Independent security research published in 2020 documented Mintegral secretly enumerating installed apps, performing click-injection fraud, and exfiltrating device data.

No response was received naming this finding. Sexual orientation, relationship data, and location of EU users co-exist in the same application as an SDK with a documented history of unauthorized data collection, transmitting to Chinese servers under PIPL with no EU adequacy decision and no stated Art. 6 or Art. 9 legal basis.

Impact: Behavioral and relationship-preference data is exposed to an ad network with a documented history of unauthorized collection and fraud, 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 for this data flow.

C3: FaceUnity biometric SDK: facial data to Chinese infrastructure, no adequacy decision

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.faceunity (619 classes), a Chinese company providing AR face-effect processing, generates a biometric representation of a natural person, GDPR Art. 9(1) special category data.

No response was received naming this finding. Transmission to FaceUnity's Chinese infrastructure has no EU adequacy decision, is subject to Chinese government access rights under PIPL and the Cybersecurity Law, and requires explicit Art. 9(2)(a) consent, none of which is confirmed. This is structurally more severe than comparable US-based biometric findings elsewhere in RFI-IRFOS's research, because no transfer mechanism at all exists between the EU and China for this category of data.

Impact: Facial biometric data is processed and transmitted to Chinese infrastructure with no EU transfer safeguard and no confirmed specific consent.

Fix: Remove FaceUnity or implement a verified Art. 44-49 mechanism, obtain explicit Art. 9(2)(a) consent, and disclose FaceUnity as a biometric processor under Art. 13(1)(e).

C4: Broken network_security_config.xml: a literal syntax error disables certificate pinning for the API gateway

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

The domain-config entry reads <domain includeSubdomains="true">"api-gateway.lovoo.com"</domain>, with literal quotation marks that never match the real hostname api-gateway.lovoo.com.

```
<domain includeSubdomains="true">"api-gateway.lovoo.com"</domain>
<!-- never matches the actual hostname api-gateway.lovoo.com -->
```

No response was received naming this finding. Because the domain value never matches, the API gateway falls through to the base config with no certificate pinning at all. Combined with C1, the attack surface compounds: traffic can be intercepted in transit by any system-trusted CA on a compromised network, and the same data is separately logged in plain text on-device by Chucker.

Impact: All traffic to Lovoo's API gateway, the entire application's core traffic, is susceptible to MITM interception by any system-trusted CA, a one-character-class typo away from working correctly.

Fix: Correct the domain-config syntax error and verify certificate pinning is actually active against a live traffic capture, not just a static config read.

H5: Development Firebase URL and API key hardcoded in the 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

firebase_database_url_dev (lovoo-dev.firebaseio.com) ships alongside the production URL, plus a hardcoded Google API key, AIzaSyAhRiD9KSCEV61_3FWCxE-Sr1_jyUWdrrs.

No response was received naming this finding. The development database may carry weaker security rules than production; both returned 'Permission denied' for unauthenticated access at time of testing, but the credentials themselves remain shipped regardless.

Impact: A development-tier backend URL and its credential are exposed in a public production release, alongside an API key enabling FCM probing.

Fix: Remove all development-environment URLs and credentials from release builds; rotate the exposed key.

H6: Seven simultaneous ad networks on a sexual-orientation data platform

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

Mintegral, AppLovin, IronSource, InMobi, Fyber/Digital Turbine, PubMatic, and MoLoco are all integrated simultaneously.

No response was received naming this finding. Simultaneous transmission of sexual orientation and relationship-preference signals, GDPR Art. 9 special category data, to seven independent commercial advertising ecosystems has no valid Art. 9(2) legal basis documented anywhere in the binary.

Impact: Sexual orientation and relationship-preference signals reach seven independent commercial ad networks simultaneously.

Fix: Consolidate ad network integrations and obtain specific Art. 9(2) consent before any special-category-adjacent signal reaches third-party advertising infrastructure.

H7: Braze marketing automation triggered on Art. 9 behavioral data

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 Braze SDK drives push, in-app, and re-engagement marketing automation, with triggers necessarily derived from sexual-preference behavioral signals on a dating platform.

No response was received naming this finding. Automated marketing based on Art. 9 data requires explicit Art. 9(2)(a) consent; legitimate interest is not available as a basis for special category data.

Impact: Marketing automation is driven by inferred sexual-preference behavioral signals with no confirmed specific consent basis.

Fix: Scope Braze triggers away from Art. 9-adjacent behavioral signals absent explicit consent.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 4(12), Art. 32	Live, ongoing plaintext logging of auth tokens and Art. 9 profile fields on-device
C2	GDPR Art. 5(1)(a), Art. 6(1), Art. 44-49	Data exposed to an ad network with a documented fraud history, no transfer safeguard
C3	GDPR Art. 9(1), Art. 44-49	Biometric facial data to Chinese infrastructure, no adequacy mechanism
C4	GDPR Art. 32(1)(a)	Certificate pinning disabled by a configuration syntax error
H5	GDPR Art. 32	Exposed development-tier credentials in a production release
H6, H7	GDPR Art. 5(1)(c), Art. 6(1), Art. 9, Art. 22	Special-category-adjacent behavioral signals reaching commercial ad and marketing infrastructure with no documented Art. 9(2) basis

Additional Findings

- H8: android.permission.MANAGE_ACCOUNTS grants access to Android AccountManager entries for other apps on the device, disproportionate to any disclosed Lovoo purpose.
- M9: LiveRamp ATS is integrated alongside a OneTrust consent management platform; whether OneTrust-collected consent actually gates LiveRamp's initialization, and whether that consent meets Art. 7 for Art. 9-adjacent data, could not be confirmed from static analysis alone.

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to privacy@lovoo.com (security@lovoo.com bounced immediately), 9 findings, bcc HmbBfDI/Austrian DSB
2026-06-28	R2 formal escalation naming the Art. 33 72-hour notification deadline as already passed; same day, the only response of any kind arrives: an automated Zendesk ticket confirmation
2026-07-03	R3, final deadline set for 2026-07-10
2026-07-24	Follow-up, 14 days past the R3 deadline, still no substantive reply
2026-09-04	Follow-up, 76 days since R1, restates the three standing questions on Chucker removal, DPO awareness, and the FaceUnity transfer mechanism
2026-09-19	Embargo closes; this report publishes

Five written notices, one automated ticket, zero substantive replies, across 91 days. All nine findings, including a live, ongoing data exposure via Chucker, stand exactly as originally reported.

Residual Risk & Recommendations

- Remove Chucker from the production build immediately; this is a live exposure, not a theoretical one, and the highest-priority item in this report regardless of its comparatively lower CVSS Base score.
- Correct the network_security_config.xml syntax error and verify pinning against a live traffic capture.
- Remove or replace Mintegral and FaceUnity, or implement verified Art. 44-49 transfer mechanisms and explicit Art. 9(2)(a) consent for both.
- Remove development-environment credentials from all release builds.
- Confirm whether an Art. 35 DPIA covers the Chucker and Mintegral findings specifically, and whether the Art. 33 notification duty triggered by C1 has been met.

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. 4, 5, 6, 9, 22, 32, 33, 35, 44-49. REF LOVOO-2026-R1.