Coordinated Security & Privacy Disclosure, Final Report

Parship (com.parship.android)

Relationship platform, ParshipMeet Group

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, REJECTED BY COUNSEL, ALL SIX FINDINGS UNRESOLVED

Target	ParshipMeet Holding GmbH / PE Digital GmbH, Speersort 10, 20095 Hamburg, Germany
Product audited	Parship for Android, com.parship.android, v10.86.0, build 2026052601
Disclosure reference	REF PARSHIP-2026-R1 / PARSHIP-FOLLOWUP-2026-09
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (P2 TheMeetGroup biometric SDK, CVSS v4.0 8.7 High) / P4 transport security scores 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 Parship Android application and identified six findings, three CRITICAL and three HIGH. The most significant: a complete biometric face-detection SDK operating under the com.themeetgroup namespace, infrastructure inherited from the 2020 acquisition that formed ParshipMeet Group, processing GDPR Art. 9 biometric data with no consent architecture visible in the binary and never disclosed to Parship users as originating from that acquisition.

Of the more than one hundred targets in RFI-IRFOS's June 2026 disclosure wave, ParshipMeet Group is among a small minority that engaged in sustained, substantive, named-contact correspondence rather than silence or generic auto-acknowledgment. That correspondence did not resolve the findings. It ended in a categorical rejection delivered first by an operations executive and then escalated to formal denial through in-house counsel, who asked RFI-IRFOS to stop contacting the company, citing the resource cost of the correspondence.

RFI-IRFOS declined that request in writing the same day, on the basis that RFI-IRFOS's own disclosure programme is run at its own cost with no funding tied to this or any specific case, and that a company's stated deadline for its own review does not pause a research programme's fixed public-disclosure clock. That deadline, 11 September 2026, set by ParshipMeet Group's own correspondence, has passed with no further reply. All six findings stand exactly as reported.

Scope: Static analysis of the publicly downloaded production Parship 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 covering both Parship and Lovoo (ParshipMeet Group and Bumble Inc. products sharing correspondence history at the time). Unlike most targets in this campaign, ParshipMeet Group engaged substantively and repeatedly: Henning Andersen (VP Platform Operations and Security) replied on 31 July 2026 confirming receipt and naming himself, Sahil Kapila (Information Security Officer), and Dr. Sophie Victoria Knebel (Senior Legal Counsel and DPO) as contacts. On 24 August 2026 he rejected all findings without addressing any of them individually. On 7 September 2026, Dr. Knebel escalated the rejection through counsel and asked RFI-IRFOS to stop contacting ParshipMeet Group, citing resource cost. RFI-IRFOS's own written notices over the same period likewise consumed RFI-IRFOS's own resources, run at its own cost with no funding tied to any specific case; that request was declined in writing the same day. ParshipMeet Group's own follow-up deadline of 11 September 2026 has now passed with no further reply.

ID	Severity	Title
P1	CRITICAL	iovation FraudForce (TransUnion): credit-bureau device fingerprinting on a relationship platform

ID	Severity	Title
P2	CRITICAL	TheMeetGroup Face Detection SDK: biometric processing inherited from a 2020 acquisition, never disclosed
P3	CRITICAL	Firebase API key hardcoded in production APK
P4	HIGH	No network_security_config.xml; certificate pinning posture unverifiable from static analysis
P5	HIGH	PubNub: private romantic messages routed through US third-party infrastructure
P6	HIGH	Selligent Marketing Cloud and Adjust: behavioral profiling on relationship data

Subject & Operator Analysis

ParshipMeet Holding GmbH and its operating entity PE Digital GmbH (Hamburg, Germany) operate Parship, a relationship platform, as part of ParshipMeet Group, formed via the 2020 acquisition of The Meet Group (MeetMe, SKOUT, Tagged, Growlr). This report's most significant finding, the TheMeetGroup biometric SDK, is a direct technical artifact of that acquisition. The Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) is the competent supervisory authority and was bcc'd or cc'd throughout this correspondence.

Findings

P1: iovation FraudForce (TransUnion): credit-bureau device fingerprinting on a relationship 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

com.iovation.mobile.android, confirmed classes FraudForceManager, FraudForceConf iguration, FraudForceConfiguration$Builder. iovation is a TransUnion product, one of the three major US credit bureaus.

ParshipMeet Group's own final position, delivered 24 August 2026 (Henning Andersen) and reaffirmed 7 September 2026 (Dr. Sophie Knebel), was a categorical statement that appropriate technical and organizational measures and contractual agreements are in place, without identifying which measure establishes a lawful basis for this specific data flow, or confirming the fingerprint activates only after consent rather than before. That specific question, put in writing on 24 August and repeated on 4 and 7 September 2026, was never answered.

Impact: Persistent device fingerprints built from hardware IDs, network data, and behavioral signals on a relationship platform are transmitted to a US credit bureau's identity graph, linking sensitive relationship-seeking behavior to commercial credit-bureau infrastructure with no stated Art. 6 basis.

Fix: Publish the specific Art. 6/7 legal basis for this data flow and the technical control ensuring the SDK activates only after consent.

P2: TheMeetGroup Face Detection SDK: biometric processing inherited from a 2020 acquisition, never disclosed

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.themeetgroup.facedetection: FaceProcessor, DetectedFace, DetectedFaceLandmark, FaceDetectionParameters. Manifest declares USE_BIOMETRIC and USE_FINGERPRINT. com.themeetgroup is the code namespace of The Meet Group (MeetMe, SKOUT, Tagged, Growlr), acquired in 2020 to form ParshipMeet Group.

This SDK is not original Parship code; it is Meet Group infrastructure that entered Parship through the acquisition. Extracting facial landmarks is processing of biometric data for unique identification under GDPR Art. 4(14), a special category under Art. 9(1) requiring explicit Art. 9(2)(a) consent. ParshipMeet Group's 24 August and 7 September responses asserted adequate measures exist without confirming, when asked directly and in writing twice, whether the Datenschutzbeauftragte was informed of this specific finding or whether an Art. 35 DPIA covers this specific integration. Neither question was answered.

Impact: Users seeking a partnership on Parship have biometric facial data processed through infrastructure originally built for unrelated social-discovery apps, with no confirmed consent architecture specific to that processing.

Fix: Confirm in writing whether an Art. 35 DPIA covers this integration, whether the DPO has reviewed it specifically, and implement explicit Art. 9(2)(a) consent before any facial landmark extraction.

P3: 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

AIzaSyBnVLqBOYSQXz8wB8oDrAJyOLuZ5nycPe8, project parship-1366, database parship-1366.firebaseio.com. The database returns 'Permission denied' for unauthenticated access, but the credential itself remains shipped in the production binary.

No Security Rules or App Check confirmation was provided in any of ParshipMeet Group's responses despite this being one of the three findings named directly, twice, in writing.

Impact: The exposed key enables FCM token enumeration against Parship's registered users and probing of any other Firebase services on the same project, independent of the database's own access rules.

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

P4: No network_security_config.xml; certificate pinning posture unverifiable from static analysis

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 in the APK. Two CA certificates in assets/ (DigiCertHighAssuranceEVRootCA.crt, entrust_g2_ca.cer) suggest a possible custom TrustManager, but its actual behavior could not be confirmed from static analysis alone.

RFI-IRFOS states plainly what was and was not verified here: the absence of the standard Android NSC pinning mechanism is confirmed; whether a custom TrustManager implementation provides equivalent protection is not, and would require dynamic testing outside this programme's static-only methodology. ParshipMeet Group's responses did not address this finding by naming the actual TrustManager behavior.

Impact: For a platform processing relationship profiles and romantic correspondence, an unverifiable TLS pinning posture leaves open the possibility of MITM interception with no confirmed client-side defense.

Fix: Publish the actual TrustManager implementation and its verification behavior, or implement standard network_security_config.xml pinning if no equivalent protection exists.

P5: PubNub: private romantic messages routed through US third-party infrastructure

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2

com.pubnub, extensive integration across multiple smali class packages, is Parship's real-time private-chat infrastructure. PubNub is a US company (San Francisco).

All private messages between Parship users, romantic correspondence and personal communication on a platform explicitly positioned on premium privacy expectations, transit and are stored on PubNub's US infrastructure. This was not addressed individually in ParshipMeet Group's responses.

Impact: Private romantic correspondence is stored on third-party US infrastructure, a data flow not disclosed to users of a platform that markets itself on elevated privacy expectations.

Fix: Disclose PubNub's role as message processor explicitly, and assess whether an Art. 44-49 transfer mechanism is in place.

P6: Selligent Marketing Cloud and Adjust: behavioral profiling on relationship 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

com.selligent.sdk triggers marketing campaigns based on in-app dating behavior; com.adjust.sdk performs ad attribution, sharing behavioral data with US-based ad-measurement infrastructure.

Not addressed individually in ParshipMeet Group's responses.

Impact: Behavioral data from a relationship-seeking context feeds marketing automation and advertising attribution infrastructure.

Fix: Scope Selligent and Adjust data collection away from relationship-preference behavioral signals, or obtain specific consent for this use.

Date	Event

Disclosure Timeline & Outcome: A Genuine Dialogue That Ended in Denial Through Counsel

Date	Event
2026-06-20	R1 sent (combined with the separate Lovoo disclosure in early correspondence), 6 findings
2026-06-28 / 07-03	Follow-ups, automated customer-service deflection pattern noted
2026-07-30	RFI-IRFOS re-engages, documents the full send history
2026-07-31	Henning Andersen (VP Platform Operations and Security) replies, confirms receipt, names Sahil Kapila (ISO) and Dr. Sophie Knebel (DPO) as contacts
2026-08-24	Andersen rejects all findings without addressing any individually: 'we have the right set of both technical and organisational measures as well as contractual agreements in place… no need to act'
2026-08-24	RFI-IRFOS responds same day: 'Alleged Is Not a Rebuttal', restates all six findings
2026-09-04	Follow-up narrows to three named artifacts and three specific questions, deadline 11 September 2026
2026-09-07	Dr. Sophie Victoria Knebel (Senior Legal Counsel and DPO) escalates: 'our review has not identified a personal data breach… we consider the matter closed from our side. Please don't contact us anymore. That consumes an enormous amount of resources.'
2026-09-07	RFI-IRFOS responds nine minutes later, same day
2026-09-19	ParshipMeet Group's own 11 September deadline, twelve days passed with no further reply; embargo closes and this report publishes

Response Pattern Atlas: P-06, Structured Denial

Dr. Knebel's message answered a question that was never asked, whether a personal data breach with a notification duty had occurred, in place of the three questions actually put in writing: a specific Art. 6/7 legal basis, whether the DPO reviewed the biometric finding specifically, and whether an Art. 35 DPIA exists for it. A categorical 'not correct' that names none of the three artifacts is an assertion, not a rebuttal. RFI-IRFOS's own reply made the point directly: naming an artifact, confirming a rotation, or producing a document would have taken ParshipMeet Group's InfoSec team less time than convening Senior Legal Counsel for a categorical denial. RFI-IRFOS's own disclosure programme runs at its own cost as well, on a fixed 90 day clock that does not pause for either side's workload, and a request to stop contacting a company mid-disclosure, ahead of that company's own stated deadline, was not something this correspondence honored on request.

ParshipMeet Group is not a silent target. It is a target that engaged, named real contacts, set its own deadlines, and ultimately declined to answer three specific, repeatedly-restated technical and procedural questions, choosing instead a categorical denial delivered through counsel. All six findings, three of them CRITICAL, stand exactly as originally reported.

Data Protection, Article by Article

Finding	Provision	Concern
P1	GDPR Art. 5(1)(c), Art. 6, Art. 44-49	Credit-bureau device fingerprinting with no stated lawful basis or transfer mechanism
P2	GDPR Art. 9(1), Art. 4(14), Art. 9(2)(a), Art. 35	Undisclosed biometric processing inherited from a corporate acquisition, DPIA status unconfirmed
P3	GDPR Art. 32	Exposed backend credential
P4	GDPR Art. 32(1)(a)	Unverifiable transport security posture
P5	GDPR Art. 5(1)(f), Art. 44-49	Undisclosed third-party US storage of private correspondence
P6	GDPR Art. 5(1)(c), Art. 9	Behavioral profiling on relationship-preference data

Residual Risk & Recommendations

- Answer, in writing, the three questions restated on 4 and 7 September 2026: the specific Art. 6/7 basis for iovation/TransUnion fingerprinting, DPO review status of the TheMeetGroup biometric SDK, and whether an Art. 35 DPIA covers it.
- Publish the actual TrustManager behavior behind the two bundled CA certificates, or implement standard certificate pinning.
- Rotate the exposed Firebase key and enable App Check.
- Disclose PubNub's role as message processor to users.
- Scope Selligent and Adjust away from relationship-preference behavioral signals absent specific consent.

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, 32, 35, 44-49. REF PARSHIP-2026-R1.