



Sicherheits- & Datenschutz-Offenlegung, Abschlussbericht

Yesim: eSIM & Mobile Internet (com.yesimmobile)

Google Consent Mode auf Granted voreingestellt, sieben Telemetrie-Anbieter inklusive Session Replay, kein EU-Vertreter; nach 89 Tagen erste Sachantwort mit Behebungsangaben zu allen drei HIGH-Befunden, vom Hersteller berichtet und nicht unabhängig geprüft

**ÖFFENTLICHE OFFENLEGUNG, 17. OKTOBER 2026, EMBARGO ERREICHT AM 29.
SEPTEMBER 2026, BEHEBUNG VOM HERSTELLER BERICHTET, NICHT
UNABHÄNGIG GEPRÜFT**

Zielunternehmen	Genesis Group AG, Bahnhofstrasse 4, 6340 Baar (Kanton Zug), Schweiz (CHE-135.623.633)
Package	com.yesimobile, Version 5.39.1 (versionCode 915)
Analysierte Plattform	Android, statische Analyse von base.apk und der arm64-Konfiguration, Flutter-Bibliothek libapp.so
Erstmeldung (R1)	2026-07-01 (REF YESIM-2026-R1-001)
Embargo-Datum	2026-09-29
Bericht veröffentlicht	2026-10-17
Gesamtschwere	HIGH
Befunde	7 (3 High, 3 Medium, 1 Low)
Korrespondenz	Mindestens 9 Sendungen von RFI-IRFOS; Support-Bot (Intercom) in drei Tickets mit wechselnden Personen-Namen, ein Abwesenheitshinweis, eine Empfangsbestätigung der Rechtsabteilung (27.07.), zwei Sachantworten der Rechtsabteilung (28.09. und 01.10.); kein Bounce
CC Behörden	DSB Österreich · EDPS · EDÖB (Schweiz)
SHA-256 (base APK)	7c90e566ad62428c8650831e89d7bb6b63bfe5a54f7733a254a12d3299e626fa

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Gegenstand & Betreiber-Kontext	5
3	Korrespondenz-Zusammenfassung	5
4	Was korrekt umgesetzt ist (Honest Positives)	5
5	Findings	6
5.1	H1: Consent Mode standardmäßig auf Granted, Auto-Init-Tracker, keine CMP .	6
5.2	H2: Sieben Telemetrie-Anbieter inklusive Amplitude Session Replay	6
5.3	H3: Übermittlung an US-Verarbeiter, kein EU-Vertreter auffindbar	7
5.4	M1: Hartcodierte API-Schlüssel und Client-Tokens	7
5.5	M2: Zwei Zahlungsdienstleister und Kartenscan per Kamera	8
5.6	M3: Breite Berechtigungen einschließlich Fine Location und AdServices	8
5.7	L1: Overlay-Berechtigung SYSTEM_ALERT_WINDOW	8
6	Impact-Analyse (Impact Analysis)	9
7	Die vollständige Kette (The Complete Chain)	9
8	Datenschutz, Artikel für Artikel (Data Protection)	9
9	Regulatorisches & rechtliches Umfeld (Regulatory)	9
10	Indicators of Compromise	10
11	Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis	10
12	Restrisiko & Empfehlungen (Residual Risk)	11

Executive Summary

Yesim ist eine eSIM- und Datenpaket-App der Genesis Group AG (Schweiz). Eine Root-Level-Analyse der Produktions-APK (Version 5.39.1) fand sieben Befunde: drei HIGH, drei MEDIUM, einen LOW.

Der Kernbefund (H1): Das Manifest setzt alle vier Google-Consent-Mode-Signale (ad_storage, ad_user_data, ad_personalization_signals, analytics_storage) auf true (granted), während Facebook, AppsFlyer und Firebase sich selbst initialisieren und keine Consent-Management-Plattform gebündelt ist. Hinzu kommen sieben Telemetrie-Anbieter, darunter Amplitude Session Replay (H2), und Übermittlungen an US-Verarbeiter ohne dokumentierte Garantien sowie ohne auffindbaren EU-Vertreter (H3).

Biometrisches KYC wurde nicht gefunden: Die Kamera dient Stripe CardScan und eSIM-QR-Codes. Das ist ein Pluspunkt gegenüber vergleichbaren eSIM-Anbietern.

Die Kommunikation lief zunächst nur über einen Support-Bot, der drei Tickets unter wechselnden Namen führte, eine User-ID verlangte und ein Ticket mit dem Hinweis schloss, es gebe keine Updates. Am 28. September, einen Tag vor dem Embargo, antwortete die Rechtsabteilung erstmals inhaltlich: Consent Mode werde nun nach tatsächlicher Wahl gesetzt, Session Replay erfasse keine Zahlungs- oder Kontobildschirme, SCC/TIA seien vorhanden, ein EU-Vertreter (Priverion Deutschland GmbH) sei benannt. Am 1. Oktober präzisierte sie: Der Consent-Mode-Fix sei im Build vom 28. September enthalten, Amplitude Session Replay sei aus den Anbietern des aktuellen Builds entfernt, der Befund vom 1. Juli habe einen früheren Build zutreffend beschrieben. Diese Angaben sind Herstellerangaben und wurden von RFI-IRFOS nicht gegen den aktuellen Build gemessen.

ID	Severity	Title
H1	HIGH	Consent Mode standardmäßig auf Granted, Auto-Init-Tracker, keine CMP
H2	HIGH	Sieben Telemetrie-Anbieter inklusive Amplitude Session Replay
H3	HIGH	Übermittlung an US-Verarbeiter, kein EU-Vertreter auffindbar
M1	MEDIUM	Hartcodierte API-Schlüssel und Client-Tokens
M2	MEDIUM	Zwei Zahlungsdienstleister und Kartenscan per Kamera
M3	MEDIUM	Breite Berechtigungen einschließlich Fine Location und AdServices
L1	LOW	Overlay-Berechtigung SYSTEM_ALERT_WINDOW

Gegenstand & Betreiber-Kontext

Yesim ist eine Marke der Genesis Group AG mit Sitz in der Schweiz. Das Kern-Backend läuft unter britischen Domains (api3.yesim.co.uk), die Schweiz und das Vereinigte Königreich haben Angemessenheitsbeschlüsse der EU. Die Art.-44-Exposition entsteht durch US-Analyse-Verarbeiter.

Als Schweizer Betreiber mit Angebot an EWR-Nutzer benötigt Genesis Group AG einen EU-Vertreter nach Art. 27 DSGVO, sofern keine Ausnahme greift.

Korrespondenz-Zusammenfassung

Die Erstmeldung ging am 1. Juli 2026 an support@yesim.app (REF YESIM-2026-R1-001), Embargo 29. September. Der Support-Bot eröffnete drei Tickets (#113194392, #113195536, #113205363) mit wechselnden Namen, verlangte eine User-ID und die Wiederholung der Anfrage von einer offiziellen Institutsadresse und schloss das erste Ticket am 2. Juli mit dem Hinweis, es habe keine Updates gegeben.

RFI-IRFOS schrieb daraufhin am 2. Juli direkt an die beiden Ansprechpersonen und an weitere Adressen, am 17. und 27. Juli sowie am 24. und 31. August erneut, ab 17. Juli mit DSB, EDPS und EDÖB im CC. Es gab einen Abwesenheitshinweis eines Empfängers (bis 21. Juli) und am 27. Juli eine Empfangsbestätigung der Rechtsabteilung (received and noted).

Am 28. September 2026 folgte die erste Sachantwort der Rechtsabteilung zu H1 bis H3, am 29. September die Antwort von RFI-IRFOS (H3 als neue Information anerkannt, H1 als zu prüfende Behauptung, H2 als direkter Widerspruch zwischen Befund und Antwort, SCC/TIA ohne Belege). Am 1. Oktober präzisierte die Rechtsabteilung (siehe Zusammenfassung); Veröffentlichung des EU-Vertreterers seit 28. September auf der Cookie-Seite, Aufnahme in die Datenschutzerklärung bis 30. Oktober angekündigt.

Was korrekt umgesetzt ist (Honest Positives)

- Kein biometrisches oder dokumentenbasiertes KYC, keine Art.-9-Verarbeitung in der Binärdatei gefunden.
- allowBackup=false, nicht debuggable, kein Klartext-Override, alle beobachteten Backend-Endpunkte HTTPS.
- Keine chinesischen, sanktionierten oder russischen Tracker trotz Gründerhintergrund.
- Zahlungen über Stripe mit hCaptcha und Geräteattestierung.
- EU-Ingest-Hosts für PostHog und Amplitude existieren und zeigen Datenresidenz-Bewusstsein.
- Die Rechtsabteilung hat die Meldung schließlich inhaltlich beantwortet, einen EU-Vertreter benannt und den Befund vom 1. Juli ausdrücklich als zutreffend für den früheren Build bezeichnet.

Findings

H1: Consent Mode standardmäßig auf Granted, Auto-Init-Tracker, keine CMP

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, 7.5

```
google_analytics_default_allow_ad_user_data: true
google_analytics_default_allow_ad_storage: true
google_analytics_default_allow_ad_personalization_signals: true
google_analytics_default_allow_analytics_storage: true
CMP-Suche (usercentrics|onetrust|didomi|UMP): 0 Treffer
```

Impact: Das Manifest setzt `ad_storage`, `ad_user_data`, `ad_personalization_signals` und `analytics_storage` auf `true`. `FacebookInitProvider`, `AppsFlyer-Install-Receiver` und `Firebase InitProvider` starten selbst, eine Consent-Management-Plattform ist nicht gebündelt. Der Standardzustand vor einer Einwilligung muss verweigert sein. Der Hersteller berichtet eine Behebung im Build vom 28. September 2026; diese Angabe wurde nicht gegen den aktuellen Build gemessen.

H2: Sieben Telemetrie-Anbieter inklusive Amplitude Session Replay

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, 7.5

```
com/appsflyer/internal (471), com/facebook/appevents (352), com/amplitude/android
(235)
sr-client-cfg.eu.amplitude.com (Session-Replay-Konfiguration)
eu.i.posthog.com + us.i.posthog.com, Segment, app-measurement.com, Sentry
```

Impact: `AppsFlyer`, `Facebook`, `Amplitude` (mit `Session-Replay-Konfiguration`), `PostHog`, `Segment`, `Firebase/GA4` und `Sentry` sind eingebunden. Für eine eSIM-Utility ist das eine dichte Telemetrie, die Art. 25 und die Empfängerangabe nach Art. 13 berührt. Der Hersteller erklärt, `Session Replay` sei im aktuellen Build entfernt und habe in dem früheren Build zwar konfigurat

H3: Übermittlung an US-Verarbeiter, kein EU-Vertreter auffindbar

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, 7.5

```
us.i.posthog.com | eu.i.posthog.com  
api2.amplitude.com | api.eu.amplitude.com  
app-measurement.com  
Kern-Backend: api3.yesim.co.uk (UK), Betreiber CH
```

Impact: Neben EU-Ingest-Hosts sind US-Endpunkte eingebunden (us.i.posthog.com, api2.amplitude.com, app-measurement.com, Facebook, AppsFlyer). Garantien (DPF, SCC, TIA) waren nicht dokumentiert, ein Art.-27-Vertreter war nicht auffindbar. Der Hersteller nennt nun Priverion Deutschland GmbH als Vertreter (veröffentlicht seit 28. September 2026) und erklärt, SCC/TIA seien vorhanden, ohne Belege.

M1: Hartcodierte API-Schlüssel und Client-Tokens

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3

```
google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Yesim /  
Genesis Group AG in R1]  
facebook_client_token: [REDACTED IN PUBLIC REPORT -- disclosed privately to Yesim /  
Genesis Group AG in R1]  
posthog_project_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Yesim /  
Genesis Group AG in R1]  
amplitude_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Yesim /  
Genesis Group AG in R1]
```

Impact: Firebase-/Google-Schlüssel, Facebook-Client-Token, PostHog-Projektschlüssel und ein Amplitude-Format-Schlüssel sind in der Binärdatei extrahierbar. Die Beweislast für Restriktionen und restriktive Rules liegt beim Betreiber.

M2: Zwei Zahlungsdienstleister und Kartenscan per Kamera

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3

Stripe CardScan und ECommPay-SDK (com.paymentpage.msdk) beobachtet.

Impact: Neben Stripe (inklusive CardScan) ist ein zweites Gateway (ECommPay) eingebunden. Empfänger müssen offengelegt und über Art. 28 gebunden sein; die On-Device-Verarbeitung der Kartenbilder ist zu bestätigen. Transparenzpunkt, kein nachgewiesener Verstoß.

M3: Breite Berechtigungen einschließlich Fine Location und AdServices

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3

Weitere Berechtigungen: CAMERA, RECORD_AUDIO (WebRTC-Telefonie), SYSTEM_ALERT_WINDOW, USE_BIOMETRIC.

Impact: ACCESS_FINE_LOCATION zusammen mit der AdServices-Familie (CUSTOM_AUDIENCE, TOPICS) geht über den Bedarf einer Datentarif-Utility hinaus und deutet auf Werbe-Zielgruppenfähigkeit.

L1: Overlay-Berechtigung SYSTEM_ALERT_WINDOW

LOW, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3

Nutzung bestätigen oder entfernen.

Impact: Die Overlay-Berechtigung ist für diese App-Klasse ungewöhnlich und missbrauchs anfällig. Wahrscheinlich dient sie der Anruf-Benachrichtigung.

Impact-Analyse (Impact Analysis)

H1 bis H3 bilden eine Kette: voreingestellte Einwilligung, dichte Telemetrie, US-Empfänger ohne belegte Garantien. Die Reichweite wird durch den Zahlungskontext der App erhöht. Die vom Hersteller berichteten Behebungen adressieren alle drei Punkte, sind aber nicht unabhängig bestätigt.

Die vollständige Kette (The Complete Chain)

Schritt 1: Erstmeldung 1. Juli 2026, Embargo 29. September. Der Support-Bot führt drei Tickets und schließt das erste.

Schritt 2: Direktnachrichten ab 2. Juli, Nachfassungen am 17. und 27. Juli, 24. und 31. August; Empfangsbestätigung der Rechtsabteilung am 27. Juli.

Schritt 3: Sachantwort der Rechtsabteilung am 28. September (Tag vor dem Embargo), Antwort von RFI-IRFOS am 29. September, Präzisierung der Rechtsabteilung am 1. Oktober.

Schritt 4: Embargo am 29. September erreicht, Veröffentlichung 18 Tage danach, 108 Tage nach der Erstmeldung. Die berichteten Behebungen sind nicht unabhängig geprüft.

Datenschutz, Artikel für Artikel (Data Protection)

Art. 6(1)(a), 7(1), 5(2) DSGVO: Standardzustand der Einwilligung (H1).

Art. 13(1)(e), 25 DSGVO: Empfänger und Datenschutz durch Voreinstellung bei sieben Anbietern (H2).

Art. 44 bis 46 und 27 DSGVO: US-Verarbeiter, Vertreter (H3).

Art. 32 DSGVO: Schlüssel und Tokens (M1).

Regulatorisches & rechtliches Umfeld (Regulatory)

Genesis Group AG ist in der Schweiz niedergelassen; für EWR-Nutzer gilt die DSGVO, Art. 27 verlangt einen EU-Vertreter. Der Hersteller nennt die Priverion Deutschland GmbH (veröffentlicht auf der Cookie-Seite seit 28. September 2026, Aufnahme in die Datenschutzerklärung bis 30. Oktober 2026 angekündigt). EDÖB, DSB und EDPS sind in Kopie informiert.

Indicators of Compromise

Technische Fundstellen der Produktions-APK. Schlüssel und Tokens sind im öffentlichen Bericht redigiert.

```
Package: com.yesimmobile 5.39.1 (915)
SHA-256 (base.apk): 7c90e566ad62428c8650831e89d7bb6b63bfe5a54f7733a254a12d3299e626fa
SHA-256 (arm64): 6cc17ebc1c7a078c96f6bdec27889211fcee866cb89c70586630eb6e483bc2b
Firebase: [REDACTED IN PUBLIC REPORT -- disclosed privately to Yesim / Genesis Group
AG in R1]
Tokens: [REDACTED IN PUBLIC REPORT -- disclosed privately to Yesim / Genesis Group
AG in R1]
Backend: api3.yesim.co.uk, pusher.yesim.co.uk, url3.yesim.guru
```

Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis

Datum	Ereignis
2026-07-01	Erstmeldung an support@yesim.app; Bot-Tickets #113194392 und #113195536
2026-07-02	Direktnachricht an die Ansprechpersonen; erstes Ticket vom Bot geschlossen
2026-07-10	Antwort im dritten Ticket #113205363
2026-07-17	Nachfassung (DSB, EDPS, EDÖB im CC); Abwesenheitshinweis eines Empfängers
2026-07-27	Nachfassung; Empfangsbestätigung der Rechtsabteilung
2026-08-24	Nachfassung
2026-08-31	Nachfassung
2026-09-28	Erste Sachantwort der Rechtsabteilung zu H1 bis H3
2026-09-29	Antwort RFI-IRFOS; Embargo erreicht
2026-10-01	Präzisierung der Rechtsabteilung
2026-10-17	Veröffentlichung dieses Berichts

Korrespondenzbilanz: mindestens neun Sendungen von RFI-IRFOS, Bot-Antworten, ein Abwesenheitshinweis, eine Empfangsbestätigung und zwei Sachantworten der Rechtsabteilung, kein Bounce. Die Behebungen zu H1 und H2 und die SCC/TIA-Angaben zu H3 sind Herstellerangaben ohne unabhängige Prüfung. Der Fall wird mit diesem Bericht geschlossen. Eine Bestätigung am aktuellen Build wird neben den Befunden vermerkt.

Restrisiko & Empfehlungen (Residual Risk)

Ob die berichteten Behebungen im ausgelieferten Build wirken, ist offen. Der EU-Vertreter ist auf der Cookie-Seite benannt, in der Datenschutzerklärung bis 30. Oktober angekündigt. Der Bericht beruht auf statischer Analyse. Laufzeitverhalten (Zeitpunkt der ersten Netzwerkeaufrufe, serverseitige Schlüsselrestriktionen, Datenregion) wurde nicht gemessen und ist als solches gekennzeichnet. Die Betreiber können diese Punkte jederzeit durch Dokumentation belegen oder widerlegen.

- Behebung von Consent Mode und Session Replay im ausgelieferten Build dokumentieren und unabhängig prüfen lassen.
 - SCC/TIA für PostHog, Amplitude, Meta, Firebase und AppsFlyer belegen.
 - EU-Vertreter wie angekündigt in der Datenschutzerklärung aufnehmen.
 - API-Schlüssel und Tokens rotieren und restringieren.
-

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Alle Befunde beruhen auf statischer Analyse der veröffentlichten Anwendung mittels öffentlich verfügbarer Werkzeuge. Es wurden keine Server, Konten oder Infrastruktur des Betreibers geprüft. Technische Nachweise sind unter Chain of Custody archiviert und werden Aufsichtsbehörden auf Anfrage zur Verfügung gestellt. Forschung durchgeführt gemäß ISO/IEC 29147, der Freiheit der Wissenschaft (Art. 17 StGG) und DSGVO Art. 89. REF YESIM-2026-R1-001.