



Sicherheits- & Datenschutz-Offenlegung, Abschlussbericht

FRITZ! Smart Home (de.avm.android.smarthome)

Firebase Analytics und Crashlytics laufen als Opt-out ab dem ersten Start, dazu globaler Klartext-Verkehr; neun Sendungen über 73 Tage ohne jede Antwort, 18 Tage nach Ablauf des Embargos

ÖFFENTLICHE OFFENLEGUNG, 17. OKTOBER 2026, EMBARGO ERREICHT AM 29. SEPTEMBER 2026, KEINE ANTWORT JEDER ART

Zielunternehmen	FRITZ! GmbH (vormals AVM GmbH), Alt-Moabit 95, 10559 Berlin
Package	de.avm.android.smarthome, Version 1.25.1 (versionCode 3290)
Analysierte Plattform	Android, statische Analyse der Produktions-APK (35,2 MB, base.apk)
Erstmeldung (R1)	2026-07-01 (REF FRITZ-2026-R1-001)
Embargo-Datum	2026-09-29
Bericht veröffentlicht	2026-10-17
Gesamtschwere	MEDIUM
Befunde	6 (3 Medium, 3 Low)
Korrespondenz	9 Nachrichten im Thread, alle 9 von RFI-IRFOS (2026-07-01 bis 2026-09-12), 0 Antworten jeder Art, kein Bounce der Hauptadresse; dsb@dsb.gv.at lieferte zeitweise nicht zu (intermittierender 554-Fehler)
CC Behörden	Berliner Beauftragte für Datenschutz und Informationsfreiheit · Österreichische DSB · EDPS
SHA-256 (base APK)	8c94b29356e43f18fe122bcca4d5ffd3967639856388c03cf29dd250a8fe719

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	M1: Firebase Analytics und Crashlytics als Opt-out aktiv ab Prozessesstart	6
5.2	M2: Zwei Google-API-Schlüssel im Klartext (Firebase und Maps)	6
5.3	M3: Globaler Klartext-Verkehr, keine Network Security Config, HTTP zu AVM-Servern	7
5.4	L1: US-Übermittlung über Google Analytics, Firebase, Crashlytics	7
5.5	L2: Veralterte SDK-Begriffe in der Datenschutzerklärung	7
5.6	L3: Hintergrundstandort für Geofencing	8
6	Impact-Analyse (Impact Analysis)	8
7	Die vollständige Kette (The Complete Chain)	8
8	Datenschutz, Artikel für Artikel (Data Protection)	8
9	Regulatorisches & rechtliches Umfeld (Regulatory)	9
10	Indicators of Compromise	9
11	Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis	9
12	Restrisiko & Empfehlungen (Residual Risk)	10

Executive Summary

FRITZ! Smart Home ist die Steuer-App zur FRITZ!Box-Smart-Home-Produktlinie. Eine Root-Level-Analyse der Produktions-APK (Version 1.25.1) fand sechs Befunde, keinen CRITICAL oder HIGH: drei MEDIUM und drei LOW.

Die App ist im Vergleich sehr zurückhaltend gebaut. Sie enthält keine Marketing-, Attributions-, Werbe- oder Session-Replay-SDKs, keine Chinese-SDKs, deaktiviert die Werbe-ID ausdrücklich, verschlüsselt die lokale Datenbank (SQLCIPHER) und scannt QR-Codes auf dem Gerät.

Der zentrale Befund (M1) ist das Opt-out-Modell: Firebase Analytics und Crashlytics sind in der Voreinstellung aktiv (Präferenz tracking_opt_out, Standardwert false) und senden an Google ab dem Prozessstart, bevor der Nutzer eine Wahl trifft. Dazu kommen zwei extrahierbare Google-API-Schlüssel (M2) und globaler Klartext-Verkehr ohne Network Security Config, einschließlich HTTP zu zwei öffentlichen AVM-Servern (M3).

Auf neun Nachrichten über 73 Tage (1. Juli bis 12. September 2026) kam keine Antwort, nicht einmal eine automatische Empfangsbestätigung.

ID	Severity	Title
M1	MEDIUM	Firebase Analytics und Crashlytics als Opt-out aktiv ab Prozessstart
M2	MEDIUM	Zwei Google-API-Schlüssel im Klartext (Firebase und Maps)
M3	MEDIUM	Globaler Klartext-Verkehr, keine Network Security Config, HTTP zu AVM-Servern
L1	LOW	US-Übermittlung über Google Analytics, Firebase, Crashlytics
L2	LOW	Veraltete SDK-Begriffe in der Datenschutzerklärung
L3	LOW	Hintergrundstandort für Geofencing

Gegenstand & Betreiber-Kontext

FRITZ! GmbH (vormals AVM) ist ein in Berlin ansässiger EU-Hersteller; Art. 27 DSGVO ist nicht einschlägig. Die App steuert Smart-Home-Geräte über die FRITZ!Box des Nutzers (REST-API, Geofencing gegen die eigene Box) und nutzt Backends unter avm.de und myfritz.de.

Die eingebettete, achtsprachige Datenschutzerklärung nennt die Verantwortliche, den Datenschutzbeauftragten (datenschutz@avm.de) und die zuständige Aufsichtsbehörde. Sie ist damit ungewöhnlich vollständig.

Korrespondenz-Zusammenfassung

Die Erstmeldung ging am 1. Juli 2026 an datenschutz@avm.de, mit DSB, EDPS und der Berliner Aufsichtsbehörde in BCC, Embargo 29. September 2026. Es folgten Nachfassungen am 6. Juli, 17. Juli, 23. Juli (erstmalig mit DSB im CC), 31. Juli, 9. August, 24. August (mit DSB und EDPS im CC), 31. August und 12. September 2026.

In diesem Zeitraum erreichte RFI-IRFOS keine Antwort, weder eine Sachantwort noch eine automatische Bestätigung. Die Nachrichten an datenschutz@avm.de wurden nie als unzustellbar zurückgewiesen.

Was korrekt umgesetzt ist (Honest Positives)

- Keine Marketing-, Attributions-, Werbe- oder Session-Replay-SDKs (kein Adjust, AppsFlyer, Branch, MoEngage, Amplitude, Sentry).
- Keine Chinese- oder sanktionierten SDKs, keine .cn- oder .ru-Endpunkte.
- Werbe-ID ausdrücklich deaktiviert (google_analytics_adid_collection_enabled=false).
- Lokale Datenbank mit SQLCipher verschlüsselt, QR-Scan on-device (MLKit).
- Erste-Partei-Backends in Deutschland, Geofencing gegen die eigene FRITZ!Box statt Hersteller-Cloud.
- Funktionierender Opt-out, vollständige Datenschutzerklärung mit benanntem DSB.
- allowBackup=false, nicht debuggable, kein RECORD_AUDIO, keine Kontakte, kein READ_PHONE_STATE.

Findings

M1: Firebase Analytics und Crashlytics als Opt-out aktiv ab Prozessstart

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

```
analytics_preferences / tracking_opt_out : getBoolean(..., false)
SmartHomeApplication.onCreate -> Tracker mit start-disabled = false
FirebaseInitProvider initOrder=100, directBootAware=true
manifest: firebase_analytics_collection_enabled nicht gesetzt
```

Impact: Die Präferenz `tracking_opt_out` hat den Standardwert `false`, der Startpfad deaktiviert die Erfassung nur bei aktivem Opt-out. `FirebaseInitProvider` initialisiert beim Prozessstart, ein Manifest-Override `firebase_analytics_collection_enabled=false` fehlt. Nicht notwendige Analyse- und Absturzdaten fließen damit vor jeder Nutzerentscheidung zu Google (`app-measurement.com`). Der Ablauf des ersten Starts ist laufzeitabhängig und wurde nicht gemessen.

M2: Zwei Google-API-Schlüssel im Klartext (Firebase und Maps)

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
FRITZ! GmbH in R1]
google_crash_reporting_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to
FRITZ! GmbH in R1]
com.google.android.geo.API_KEY: [REDACTED IN PUBLIC REPORT -- disclosed privately to
FRITZ! GmbH in R1]
```

Impact: Ein Firebase-/Crash-Reporting-Schlüssel und ein Maps-Schlüssel sind in `strings.xml` beziehungsweise im Manifest extrahierbar. Ohne Restriktionen drohen Quota- und Abrechnungserschöpfung. Ob serverseitige Restriktionen bestehen, ist nicht geprüft.

M3: Globaler Klartext-Verkehr, keine Network Security Config, HTTP zu AVM-Servern

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

```
AndroidManifest.xml: android:usesCleartextTraffic="true"
res/xml: keine network_security_config.xml
http://juis.avm.de, http://jason.avm.de
```

Impact: Das Manifest setzt usesCleartextTraffic=true ohne Network Security Config und ohne Pinning. Zwei öffentliche AVM-Server (juis.avm.de, jason.avm.de) werden per HTTP angesprochen. Klartext zur lokalen FRITZ!Box ist legitim, globaler Klartext und HTTP zu öffentlichen Servern nicht.

L1: US-Übermittlung über Google Analytics, Firebase, Crashlytics

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

Offengelegt und auf einem Angemessenheitspfad begründet.

Impact: Die Datenschutzerklärung nennt die Übermittlung an Google-Server in den USA und stützt sie auf SCC und Angemessenheitsbeschluss. Der Mechanismus trägt weitgehend; offen bleibt, dass die Übermittlung wegen M1 vor der Einwilligung beginnt.

L2: Veraltete SDK-Begriffe in der Datenschutzerklärung

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

Aktualisierung auf den ausgelieferten Stack erforderlich.

Impact: Die Erklärung nennt Google Fabric und anonymizelp, tatsächlich verbaut sind Firebase Crashlytics und GA4. Die Transparenzangabe beschreibt einen früheren Stand.

L3: Hintergrundstandort für Geofencing

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

Hinweis, kein Verstoß.

Impact: ACCESS_BACKGROUND_LOCATION mit Geofencing-Komponenten für Anwesenheitsautomation, ausgeführt gegen die eigene FRITZ!Box. Legitime Funktion, Heimkoordinaten sind personenbezogen und brauchen klare Zweck- und Speicherangaben (in der Erklärung vorhanden).

Impact-Analyse (Impact Analysis)

Die Gesamtschwere ist MEDIUM. Die Reichweite von M1 ist durch den Produktkontext erhöht: eine Marke, die auf lokale Datenhaltung setzt, sendet Telemetrie ab dem ersten Start an Google. Die übrigen Befunde sind Härtings- und Transparenzpunkte.

Die vollständige Kette (The Complete Chain)

Schritt 1: Erstmeldung 1. Juli 2026 an datenschutz@avm.de, Embargo 29. September.

Schritt 2: Acht weitere Nachfassungen bis 12. September, ab 23. Juli mit DSB im CC, ab 24. August mit DSB und EDPS.

Schritt 3: Keine Antwort jeder Art, auch keine automatische.

Schritt 4: Embargo am 29. September erreicht, Veröffentlichung 18 Tage danach, 108 Tage nach der Erstmeldung.

Datenschutz, Artikel für Artikel (Data Protection)

Art. 6(1), 7 DSGVO und § 25 TTDSG: Einwilligungsmodell für Firebase und Crashlytics (M1).

Art. 32 DSGVO: API-Schlüssel (M2) und Klartext-Verkehr (M3).

Art. 44 bis 49 DSGVO: Übermittlung an Google in den USA (L1).

Art. 13 DSGVO: aktuelle Beschreibung des ausgelieferten Stacks (L2).

Regulatorisches & rechtliches Umfeld (Regulatory)

Verantwortliche ist die FRITZ! GmbH, Berlin. Zuständige Aufsichtsbehörde laut eigener Erklärung ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit, die in BCC informiert wurde. Eine Datenschutz-Folgenabschätzung nach Art. 35 für Hintergrundstandort und Anwesenheitserkennung wurde angefragt und nicht beantwortet.

Indicators of Compromise

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

```
Package: de.avm.android.smarthome 1.25.1 (3290)
SHA-256: 8c94b29356e43f18fe122bcca4d5ffd3967639856388c03cf29dd250a8fe719
Firebase: [REDACTED IN PUBLIC REPORT -- disclosed privately to FRITZ! GmbH in R1]
Backends: api.avm.de, gateway.myfritz.de, assets.avm.de, http://juis.avm.de, http://jason.avm.de, app-measurement.com
```

Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis

Datum	Ereignis
2026-07-01	Erstmeldung an datenschutz@avm.de (BCC DSB, EDPS, Berliner Aufsicht)
2026-07-06	Nachfassung 1
2026-07-17	Nachfassung 2
2026-07-23	Nachfassung 3 (DSB im CC)
2026-07-31	Nachfassung 4
2026-08-09	Nachfassung 5
2026-08-24	Nachfassung 6 (DSB, EDPS im CC)
2026-08-31	Nachfassung 7
2026-09-12	Nachfassung 8
2026-09-29	Embargo erreicht
2026-10-17	Veröffentlichung dieses Berichts

Korrespondenzbilanz: neun Sendungen von RFI-IRFOS, null Antworten jeder Art, kein Bounce der Hauptadresse. Der Fall wird mit diesem Bericht geschlossen. Eine nachträgliche Antwort wird neben den Befunden vermerkt.

Restrisiko & Empfehlungen (Residual Risk)

Die Befunde sind zum Berichtsdatum nicht als behoben dokumentiert. Das Risiko ist gering bis mittel; die App ist im Marktvergleich zurückhaltend gebaut. Der Bericht beruht auf statischer Analyse. Laufzeitverhalten (Zeitpunkt der ersten Netzwerkaufrufe, serverseitige Schlüsselrestriktionen, Datenregion) wurde nicht gemessen und ist als solches gekennzeichnet. Die Betreiber können diese Punkte jederzeit durch Dokumentation belegen oder widerlegen.

- Firebase Analytics und Crashlytics vor der Einwilligung deaktivieren (firebase_analytics_collection_enabled=false, Opt-in).
 - Google-API-Schlüssel per Paket und Signatur beschränken.
 - Network Security Config mit Klartext nur für lokale Box-Domains, TLS für avm.de und myfritz.
 - Datenschutzerklärung auf Firebase Crashlytics und GA4 aktualisieren.
-

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 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 FRITZ-2026-R1-001.