



Sicherheits- & Datenschutz-Offenlegung, Abschlussbericht

Red Bull MOBILE eSIM (com.redbull.android.esim)

Vier Tracking- und Marketing-Anbieter starten über Auto-Init-ContentProvider ohne jede Consent-Management-Plattform, dazu ein US-Backend für EU-Abonnenten; Menschen bei A1 antworteten, die vier Sachfragen blieben unbeantwortet, 18 Tage nach Ablauf des Embargos

**ÖFFENTLICHE OFFENLEGUNG, 17. OKTOBER 2026, EMBARGO ERREICHT AM 29.
SEPTEMBER 2026, SACHFRAGEN UNBEANTWORTET**

Zielunternehmen	A1 Telekom Austria AG, Wien (laut Datenschutzhinweis des Produkts Verantwortliche); Plattform: WNDR (White-Label, Microsoft Azure)
Package	com.redbull.android.esim, Version 1.7.20 (versionCode 240)
Analysierte Plattform	Android, statische Analyse der Produktions-APK (22,7 MB, einzelne base.apk)
Erstmeldung (R1)	2026-07-01 (REF RBMESIM-2026-R1-001)
Embargo-Datum	2026-09-29
Bericht veröffentlicht	2026-10-17
Gesamtschwere	CRITICAL
Befunde	5 (1 Critical, 2 High, 1 Medium, 1 Low)
Korrespondenz	6 Sendungen von RFI-IRFOS zu diesem Fall (2026-07-01 bis 2026-09-03), 3 Antworten von Herrn Mag. Paulhart (A1) am 2026-07-02, 2026-07-03 und 2026-08-03, keine inhaltliche Antwort auf die Sachfragen, kein Bounce
CC Behörden	Österreichische Datenschutzbehörde (DSB) · Europäischer Datenschutzbeauftragter (EDPS)
SHA-256 (base APK)	48edcd240e8d2c63bc74abfa809cce3348edafdca2ecd471ea385b7cf1a cb61a

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)	6
5	Findings	6
5.1	C1: Vier-Anbieter-Tracking startet über Auto-Init ohne Consent-Management-Plattform	6
5.2	H1: Firebase-/Google-API-Schlüssel im Klartext in strings.xml	7
5.3	H2: Adjust-Attribution mit Werbe-ID, nativer Signatur und Install-Referrer	7
5.4	M1: US-Backend für EU-Abonnenten, kein EU-Vertreter in der Binärdatei	8
5.5	L1: Keine Network Security Config, Zertifikats-Pinning nicht nachweisbar	8
6	Impact-Analyse (Impact Analysis)	8
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

Red Bull MOBILE eSIM ist eine eSIM-Selbstbedienungs-App, die eSIM-Profile, Teilnehmerkennungen und Prepaid-Abwicklung verwaltet. Eine Root-Level-Analyse der Produktions-APK (Version 1.7.20) ergab fünf Befunde: einen CRITICAL, zwei HIGH, einen MEDIUM und einen LOW.

Der Kernbefund betrifft den Zeitpunkt, nicht den Umfang der Berechtigungen. Die App verlangt zur Laufzeit wenig (keine Kamera, kein Standort, kein Mikrofon, keine Kontakte), startet aber vier unabhängige Telemetrie- und Marketing-Anbieter (Firebase Analytics, automatisch aktiviertes Crashlytics, Adjust mit Werbe-ID, Braze) über Android-Auto-Init-ContentProvider, und liefert keine Consent-Management-Plattform mit. Es gibt weder OneTrust, Didomi, Usercentrics noch Google UMP in der Binärdatei. Die einzigen Consent-Bezüge sind lesende IABTCF-Schlüssel von Firebase, die ohne CMP nie beschrieben werden.

Hinzu kommen ein im Klartext extrahierbarer Firebase-/Google-API-Schlüssel (H1), die Adjust-Attribution mit Werbe-ID und Install-Referrer (H2) und ein Subscriber-Backend unter einer US-Domain ohne benannten EU-Vertreter in der Binärdatei (M1). Braze ist als einziger Anbieter korrekt auf das EU-Cluster Frankfurt festgelegt.

Die Erstmeldung erreichte A1 am 1. Juli 2026. Die Rechtsfunktion wandte zunächst einen möglichen Betrugsversuch ein, die Echtheit wurde am selben Tag belegt. Danach antwortete Herr Mag. Paulhart dreimal persönlich (Eingang bestätigt, Prüfung eingeleitet, am 3. August: interne Prüfung noch im Gange). Die vier Sachfragen vom 3. September (Prüfzuordnung, Rechtsgrundlage der vier Anbieter, DSFA, Drittlandübermittlung) blieben bis zur Veröffentlichung unbeantwortet.

ID	Severity	Title
C1	CRITICAL	Vier-Anbieter-Tracking startet über Auto-Init ohne Consent-Management-Plattform
H1	HIGH	Firebase-/Google-API-Schlüssel im Klartext in strings.xml
H2	HIGH	Adjust-Attribution mit Werbe-ID, nativer Signatur und Install-Referrer
M1	MEDIUM	US-Backend für EU-Abonnenten, kein EU-Vertreter in der Binärdatei
L1	LOW	Keine Network Security Config, Zertifikats-Pinning nicht nachweisbar

Gegenstand & Betreiber-Kontext

Red Bull MOBILE ist eine Mobilfunkmarke im Betrieb der A1 Telekom Austria AG. Die eSIM-App läuft auf der White-Label-Plattform WNDR (interner Build-Name WndrApp), deren Subscriber-Backend unter einer .us-Domain auf Microsoft Azure erreichbar ist. Die App verarbeitet Telekommunikationskennungen (EID, ICCID, MSISDN, eSIM-Aktivierungs-codes) und Zahlungsabläufe.

Die Verantwortliche ist laut Datenschutzhinweis des Produkts die A1 Telekom Austria AG. Eine Impressums- oder Rechtsträgerangabe ist in der Binärdatei nicht enthalten, die Datenschutzerklärung wird zur Laufzeit nachgeladen.

Korrespondenz-Zusammenfassung

Die Erstmeldung ging am 1. Juli 2026 an datenschutz@a1.at, mit der österreichischen Datenschutzbehörde und dem EDPS in BCC, Embargo 29. September 2026. Am selben Tag erkundigte sich Herr Mag. Paulhart (A1) nach der Echtheit der Nachrichten und sprach von einem möglichen Betrugsversuch. RFI-IRFOS bestätigte die Echtheit (Vereins- und Gewerberegisternummern, Behörden im CC) und verwies auf den kostenlosen, bedingungslosen Charakter der Offenlegung.

Am 2. Juli 2026 antwortete Herr Paulhart persönlich: Eingang der Mails zu Mein A1, yesss! und der Red Bull Mobile App bestätigt, eine Überprüfung sei eingeleitet. Am 3. Juli bedankte er sich für die Zusammenfassung. Am 3. August schrieb er, die interne Prüfung sei noch im Gange und bat um Geduld. Die Antwort nahm nicht konkret auf Red Bull MOBILE eSIM Bezug.

RFI-IRFOS fragte am 4. August nach, ob die Prüfung alle drei Marken oder Red Bull MOBILE eSIM gesondert umfasst, und stellte am 3. September vier Sachfragen mit Frist 17. September 2026. Auf beides erfolgte keine Antwort. Es gab nie einen Bounce. Am 19. September erhielt A1 eine Veröffentlichungsmitteilung zum Parallelfall Mein A1 (REF MEINA1-2026-R1), die diesen Fall nicht abschloss.

Was korrekt umgesetzt ist (Honest Positives)

- Berechtigungsumfang ist schlank: keine Kamera, kein Standort, kein Mikrofon, keine Kontakte.
- Kein biometrischer KYC-Stack und keine Chinese-SDK-Komponenten (Tencent, ByteDance, Alibaba, Baidu, Mintegral), keine .cn-Endpunkte.
- Braze ist ausdrücklich auf das EU-Cluster Frankfurt festgelegt (sdk.fra-02.braze.eu).
- Menschliche Ansprechperson bei A1 antwortete mehrfach persönlich und höflich.

Findings

C1: Vier-Anbieter-Tracking startet über Auto-Init ohne Consent-Management-Plattform

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.0

```
FirebaseInitProvider          initOrder=100, directBootAware=true
firebase_crashlytics_collection_enabled = true
com.adjust.sdk.SystemLifecycleContentProvider (Auto-Init)
Braze: FCM-Push, In-App-Messaging, Content Cards, Flush-Receiver
Permissions: AD_ID, ACCESS_AD SERVICES_ATTRIBUTION, ACCESS_AD SERVICES_AD_ID
CMP-Suche (onetrust|didomi|usercentrics|sourcepoint|UserMessagingPlatform): 0 Treffer
```

Beobachteter Fakt: Vier Anbieter sind beim Prozessstart registriert, keine CMP vorhanden. Rechtliche Schlussfolgerung: Eine Einwilligung vor Beginn der nicht notwendigen Verarbeitung ist unter diesen Bedingungen nicht nachweisbar (Art. 7(1)); die Beweislast liegt nach Art. 5(2) beim Betreiber. Ob jeder SDK beim ersten Start tatsächlich sendet, ist laufzeitabhängig und wurde nicht gemessen.

Impact: RFI-IRFOS blast-radius escalation: von HIGH/8.0 auf CRITICAL angehoben, weil die Telemetrie in einer Telekommunikations-App läuft, die EID, ICCID, MSISDN und eSIM-Codes verwaltet, und weil der Auto-Init-Mechanismus jede Einwilligung strukturell ausschließt. Firebase Analytics, Crashlytics (collection_enabled=true), Adjust und Braze sind über Content-Provider und Services beim Prozessstart registriert, eine Consent-Management-Plattform ist nicht gebündelt. Die Architektur ist aus der Binärdatei bestätigt.

H1: Firebase-/Google-API-Schlüssel im Klartext in strings.xml

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_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to A1
Telekom Austria / Red Bull MOBILE eSIM in R1]
google_crash_reporting_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to
A1 Telekom Austria / Red Bull MOBILE eSIM in R1]
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to
A1 Telekom Austria / Red Bull MOBILE eSIM in R1]
```

Impact: Ein funktionsfähiger Firebase-/Google-API-Schlüssel samt Projektkoordinaten ist aus jeder installierten APK extrahierbar. Ohne serverseitige Restriktionen (Paket, Signatur, Quota, App Check) ermöglicht das Quota- und Abrechnungerschöpfung gegen den Betreiber und, bei fehlerhaften Rules, Datenzugriff. Die Beweislast für korrekte Restriktionen liegt beim Betreiber.

H2: Adjust-Attribution mit Werbe-ID, nativer Signatur und Install-Referrer

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/adjust/sdk/Adjust, AdjustConfig, AdjustAttribution
libsigner.so: Java_com_adjust_sdk_sig_NativeLibHelper_nSign
BIND_GET_INSTALL_REFERRER_SERVICE, AD_ID, ACCESS_ADSERVICES_AD_ID
```

Impact: Die App enthält eine vollständige Werbe-Attributionskette: Adjust-SDK, native Request-Signatur (libsigner.so), Endpunkte app.adjust.com, ssrv.adjust.com, subscription.adjust.com, Google- und Huawei-Install-Referrer sowie AD_ID. Werbe-Attribution ist nicht notwendige Verarbeitung und benötigt vorherige Einwilligung; ohne CMP existiert kein erkennbarer Mechanismus dafür. Die Huawei-Referenzen sind Adjust-Standardcode und kein Chinese-SDK-Befund.

M1: US-Backend für EU-Abonnenten, kein EU-Vertreter in der Binärdatei**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**

API-Basis: <https://esim.redbullmobile.us/api/v1/> (US-TLD)
Plattform: wandr.azurewebsites.net (Microsoft Azure)
Braze: sdk.fra-02.braze.eu (EU-Cluster, korrekt)

Impact: Das Subscriber-Backend liegt unter einer US-Domain auf Azure, Firebase und Adjust routen zu US-Endpunkten. Ob EU-Nutzer regional geroutet werden, ist statisch nicht feststellbar. Die Drittlandübermittlung erfordert Garantien (SCC, TIA); ein EU-Vertreter oder Rechtsträger ist in der App nicht benannt.

L1: Keine Network Security Config, Zertifikats-Pinning nicht nachweisbar**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**

res/xml/network_security_config.xml: nicht vorhanden
usesCleartextTraffic: nicht gesetzt (Plattform-Default: blockiert)

Impact: Die App definiert keine Network Security Config und kein Zertifikats-Pinning. Mit targetSdk 35 blockiert die Plattform Klartext-HTTP standardmäßig; es handelt sich um eine Härtungslücke, keinen aktiven Verstoß.

Impact-Analyse (Impact Analysis)

C1 ist der schwerwiegendste Befund, weil er eine Telekommunikations-App betrifft, in der Teilnehmerkennungen mit einer Werbe-ID zusammentreffen können, ohne dass eine Einwilligung eingeholt werden kann. H1 und H2 verstärken sich gegenseitig: derselbe Auto-Init-Pfad, derselbe fehlende Consent-Gate.

Die vollständige Kette (The Complete Chain)

Schritt 1: Erstmeldung am 1. Juli 2026 an datenschutz@a1.at, Embargo 29. September 2026.

Schritt 2: Echtheitsrückfrage und Bestätigung am 1. Juli, Zusammenfassung der drei A1-Fälle am 2. Juli.

Schritt 3: Drei persönliche Antworten von Herrn Paulhart (2. Juli, 3. Juli, 3. August), zuletzt mit dem Hinweis, die Prüfung laufe noch.

Schritt 4: Rückfrage am 4. August und vier Sachfragen am 3. September (Frist 17. September), beide ohne Antwort.

Schritt 5: Embargo am 29. September erreicht, Veröffentlichung 18 Tage danach, 108 Tage nach der Erstmeldung.

Datenschutz, Artikel für Artikel (Data Protection)

Art. 6(1) und Art. 7(1) DSGVO: Rechtsgrundlage und nachweisbare Einwilligung vor dem Start von Firebase, Crashlytics, Adjust und Braze (C1, H2).

Art. 5(2) DSGVO: Der Betreiber muss nachweisen können, dass vor der Einwilligung nichts gesendet wird.

Art. 32 DSGVO: Extrahierbarer API-Schlüssel (H1) und fehlendes Pinning (L1).

Art. 44, 46 und 27 DSGVO: US-Backend, Azure-Plattform, fehlender EU-Vertreter in der App (M1).

Regulatorisches & rechtliches Umfeld (Regulatory)

Verantwortliche ist laut Datenschutzhinweis die A1 Telekom Austria AG, zuständige Aufsichtsbehörde ist die österreichische Datenschutzbehörde (DSB). Telekommunikationsspezifisch gilt zusätzlich das TKG 2021. Die DSB und der EDPS standen von Beginn an in Kenntnis.

Die Verantwortlichkeit von A1 und die Rolle des Plattformbetreibers WNDR (Auftragsverarbeitung nach Art. 28) sind offene Fragen, die A1 beantworten kann.

Indicators of Compromise

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

```
Package:    com.redbull.android.esim 1.7.20 (240)
SHA-256:    48edcd240e8d2c63bc74abfa809cce3348edafdc2ecd471ea385b7cflacb61a
Firebase:   [REDACTED IN PUBLIC REPORT -- disclosed privately to A1 Telekom Austria /
            Red Bull MOBILE eSIM in R1]
Backend:    esim.redbullmobile.us, link.esim.redbullmobile.com, wndr.azurewebsites.net
Adjust:     app.adjust.com, ssrv.adjust.com, subscription.adjust.com, gdpr.adjust.com
Braze:      sdk.fra-02.braze.eu
```

Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis

Datum	Ereignis
2026-07-01	Erstmeldung an datenschutz@a1.at (BCC DSB, EDPS); Echtheitsrückfrage und Bestätigung
2026-07-02	Antwort Paulhart: Eingang bestätigt, Überprüfung eingeleitet; Zusammenfassung der drei A1-Fälle
2026-07-03	Antwort Paulhart: Dank für die Zusammenfassung
2026-07-27	Statuscheck (primär Mein A1)
2026-08-03	Antwort Paulhart: interne Prüfung im Gange, Bitte um Geduld
2026-08-04	Rückfrage zur Prüfzuordnung, unbeantwortet
2026-09-03	Vier Sachfragen, Frist 17. September, unbeantwortet
2026-09-29	Embargo erreicht
2026-10-17	Veröffentlichung dieses Berichts

Korrespondenzbilanz: sechs Sendungen von RFI-IRFOS, drei persönliche Antworten von A1 ohne inhaltliche Stellungnahme zu C1, H1, H2 oder M1, kein Bounce. Der Fall wird mit diesem Bericht geschlossen. Eine nachträgliche inhaltliche Antwort wird neben den Befunden vermerkt.

Restrisiko & Empfehlungen (Residual Risk)

Alle fünf Befunde sind zum Berichtsdatum nicht als behoben dokumentiert. A1 hat weder eine Behebung noch eine Gegenposition mitgeteilt. 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.

- Consent-Management-Plattform einbinden und Firebase, Crashlytics, Adjust und Braze erst nach Einwilligung initialisieren (Auto-Init per Manifest abschalten).
 - Firebase-/Google-API-Schlüssel serverseitig auf Paket und Signatur beschränken, App Check aktivieren, Firebase-Rules prüfen.
 - Datenregion der Subscriber-Daten für EU-Nutzer dokumentieren; SCC/TIA für US-Endpunkte; Rolle von WNDR nach Art. 28 dokumentieren; EU-Vertreter oder Rechtsträger in der App benennen.
 - Network Security Config mit Pinning ergänzen.
-

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 RBMESIM-2026-R1-001.