



Sicherheits- & Datenschutz-Offenlegung, Abschlussbericht

SWIplus (ch.swissinfo.android)

Drei Attributions-SDKs, comScore und Facebook in der Nachrichten-App eines gebührenfinanzierten öffentlichen Rundfunks; die SRG bestritt den Zugang der Erstmeldung und erkannte die Befunde nicht an, beantwortete keine der Fragen, 18 Tage nach Ablauf des Embargos

**ÖFFENTLICHE OFFENLEGUNG, 17. OKTOBER 2026, EMBARGO ERREICHT AM 29.
SEPTEMBER 2026, BEFUNDE VON DER SRG NICHT ANERKANNT, FRAGEN
UNBEANTWORTET**

Zielunternehmen	SRG SSR (Schweizerische Radio- und Fernsehgesellschaft), Bern; Betreiber der App: SWI swissinfo.ch
Package	ch.swissinfo.android, Version 6.8.1 (versionCode 895)
Analysierte Plattform	Android, statische Analyse der Produktions-APK (base.apk)
Erstmeldung (R1)	2026-07-01 (REF SWIPLUS-2026-R1-001)
Embargo-Datum	2026-09-29
Bericht veröffentlicht	2026-10-17
Gesamtschwere	HIGH
Befunde	5 (3 High, 1 Medium, 1 Low)
Korrespondenz	8 Sendungen von RFI-IRFOS (2026-07-01 bis 2026-09-03), 2 Antworten der SRG Datenschutz/Rechtsdienst (2026-07-31 und 2026-08-18), keine inhaltliche Antwort auf die Fragen, kein Bounce
CC Behörden	DSB Österreich · EDPS · EDÖB (Schweiz)
SHA-256 (base APK)	915a2da9fccb0ade70f8eb7e1cc02393f007476b79fe99aa8dc31af44f1606d0

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: Kommerzielle Attributions- und Reichweitenmessung in einer News-App des öffentlichen Rundfunks	6
5.2	H2: Auto-Init von Facebook und Firebase vor dem Einwilligungsbildschirm . .	6
5.3	H3: Privacy-Sandbox-AdServices, Werbe-ID und Install-Referrer	7
5.4	M1: Google-/Firebase-API-Schlüssel im Klartext	7
5.5	L1: Keine App-Network-Security-Config, kein Pinning	7
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)	8
10	Indicators of Compromise	9
11	Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis	9
12	Restrisiko & Empfehlungen (Residual Risk)	10

Executive Summary

SWIplus ist die Mobile-App von SWI swissinfo.ch, dem internationalen Dienst der SRG SSR, finanziert über die Schweizer Haushaltsabgabe. Eine Root-Level-Analyse der Produktions-APK (Version 6.8.1) fand fünf Befunde: drei HIGH, einen MEDIUM, einen LOW.

Die App bündelt einen vollständigen kommerziellen Werbetech-Stack: Facebook SDK, Firebase/Crashlytics, AppsFlyer, Adjust, Singular und comScore, dazu die komplette Android-Privacy-Sandbox-Berechtigungsfamilie ACCESS_AD_SERVICES, die Werbe-ID und den Install-Referrer. Facebook und Firebase initialisieren über ContentProvider beim Prozessstart, noch bevor ein Einwilligungsbildschirm erscheinen kann. Ein Usercentrics-CMP ist vorhanden, das ist die richtige Kontrolle; offen ist, ob er die Auto-Init-SDKs tatsächlich steuert.

Bei Nachrichteninhalten können Nutzungsprofile Rückschlüsse auf politische Meinungen erlauben (Art. 9 DSGVO). Drei dedizierte Attributions-SDKs in einer News-App eines öffentlichen Rundfunks werfen deshalb Fragen der Zweckbindung auf.

Die SRG antwortete zweimal: am 31. Juli (Eingang bestätigt, die Erstmeldung vom 1. Juli sei in den genannten Postfächern nicht auffindbar) und am 18. August (Zustellnachweis nicht als Nachweis anerkannt, Prämissen und Befunde nicht anerkannt, zu den Fragen bestehe keine Veranlassung zur Stellungnahme). Eine inhaltliche Beantwortung der Fragen gab es nicht.

ID	Severity	Title
H1	HIGH	Kommerzielle Attributions- und Reichweitenmessung in einer News-App des öffentlichen Rundfunks
H2	HIGH	Auto-Init von Facebook und Firebase vor dem Einwilligungsbildschirm
H3	HIGH	Privacy-Sandbox-AdServices, Werbe-ID und Install-Referrer
M1	MEDIUM	Google-/Firebase-API-Schlüssel im Klartext
L1	LOW	Keine App-Network-Security-Config, kein Pinning

Gegenstand & Betreiber-Kontext

SWI swissinfo.ch ist der internationale Dienst der SRG SSR mit Sitz in Bern. Die Schweiz ist Drittland; die DSGVO gilt für EWR-Nutzer, die Schweizer Aufsicht ist der EDÖB. Eine Datenschutzkontaktangabe ist in der App nicht enthalten, die SRG-Datenschutzstelle wurde über datenschutz@srgssr.ch und info@srgssr.ch angeschrieben.

Korrespondenz-Zusammenfassung

Die Erstmeldung ging am 1. Juli 2026 um 09:09 UTC an datenschutz@srgssr.ch und info@srgssr.ch, mit EDÖB, DSB und EDPS in BCC, Embargo 29. September. Es folgten Nachfassungen am 6., 17., 23. und 31. Juli.

Am 31. Juli bestätigte die SRG Datenschutz den Eingang der Nachricht vom 31. Juli und teilte mit, eine Meldung vom 1. Juli sei in den genannten Postfächern bislang nicht auffindbar gewesen, und bat um Zustellnachweise. RFI-IRFOS lieferte am 15. August Versandzeitpunkt, Betreff, Nachrichten-ID und den Umstand, dass keine Unzustellbarkeitsmeldung einging.

Am 18. August antwortete die SRG: Die Angaben zum angeblichen Versand seien kein Nachweis des Zugangs, zu den wiederholt gestellten Fragen bestehe keine Veranlassung zur Stellungnahme, die Prämissen würden nicht anerkannt, die Eingabe vermische technische und rechtliche Aspekte, einzelne Fragen beträfen interne Prüfungen, auf die Dritte keinen Auskunftsanspruch hätten, und die Befunde seien nicht belegt. Die SRG verwies außerdem auf in der Eingabe enthaltene Beratungsangebote. Weitere Stellungnahmen behielt sie sich vor.

RFI-IRFOS antwortete am 18. August mit dem Zustellnachweis (Anhang) und am 3. September mit einer Fristerinnerung (Frist 25. August). Darauf folgte keine weitere Antwort. Die Befunde sind Beobachtungen aus der Binärdatei, jeder Befund trennt beobachteten Fakt und Schlussfolgerung, Laufzeitfragen sind als nicht gemessen gekennzeichnet. Der veröffentlichte Bericht enthält keine Angebote.

Was korrekt umgesetzt ist (Honest Positives)

- Usercentrics-CMP ist gebündelt, die richtige Kontrolle; ob er die Auto-Init-SDKs steuert, ist die offene Frage.
- `allowBackup=false`.
- `targetSdk 36`, die Plattform blockiert damit Klartext-HTTP standardmäßig.
- Keine chinesischen oder sanktionierten SDKs gefunden, Treffer für tencent, baidu, amap und getui waren Fehltreffer ohne zugehörige Paketpfade.

Findings

H1: Kommerzielle Attributions- und Reichweitenmessung in einer News-App des öffentlichen Rundfunks

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, AppsFlyer, Singular, com/comscore, com/google/firebase, crashlytics  
com.facebook.internal.FacebookInitProvider (AndroidManifest.xml)
```

Impact: Die Binärdatei enthält Adjust, AppsFlyer, Singular (Install-Attribution), comScore (Publikumsmessung), Facebook SDK sowie Firebase und Crashlytics. Drei Attributions-SDKs plus Reichweitenmessung sind für die Auslieferung von Journalismus unverhältnismäßig und eine Zweckbindungsfrage. Nachrichtennutzung kann politische Meinungen offenlegen (Art. 9).

H2: Auto-Init von Facebook und Firebase vor dem Einwilligungsbildschirm

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.facebook.internal.FacebookInitProvider  
com.google.firebase.provider.FirebaseInitProvider  
io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingInitProvider
```

Impact: FacebookInitProvider, FirebaseInitProvider und der Flutter-Firebase-Messaging-Provider initialisieren in ContentProvider.onCreate() beim Prozessstart, vor jeder Oberfläche. Der Mechanismus ist aus der Binärdatei bestätigt; ob vor der Einwilligung Netzwerkaufrufe erfolgen, ist laufzeitabhängig und wurde nicht gemessen.

H3: Privacy-Sandbox-AdServices, Werbe-ID 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

```
android.permission.ACCESS_AD_SERVICES_AD_ID / _ATTRIBUTION / _CUSTOM_AUDIENCE / _TOPICS
com.google.android.gms.permission.AD_ID
BIND_GET_INSTALL_REFERRER_SERVICE
AdvertisingIdClient.getAdvertisingIdInfo
```

Impact: Die App deklariert ACCESS_AD_SERVICES_AD_ID, _ATTRIBUTION, _CUSTOM_AUDIENCE und _TOPICS sowie AD_ID und den Install-Referrer-Dienst, und enthält Code zum Auslesen der Werbe-ID. CUSTOM_AUDIENCE und TOPICS sind interessenbasierte Werbe-APIs und zeigen Zielgruppenfähigkeit. Die tatsächliche Übertragung ist laufzeitabhängig.

M1: Google-/Firebase-API-Schlüssel im Klartext

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 SRG SSR in R1]
```

Impact: Ein Schlüssel samt Projektkoordinaten ist in strings.xml extrahierbar. Quota- und Abrechnungerschöpfung sind ohne Restriktionen möglich.

L1: Keine App-Network-Security-Config, kein Pinning

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

usesCleartextTraffic nicht gesetzt.

Impact: Es gibt keine networkSecurityConfig und kein Zertifikats-Pinning. Klartext ist plattformseitig geblockt; Härtungslücke, kein Verstoß.

Impact-Analyse (Impact Analysis)

H1 bis H3 verstärken sich: derselbe Auto-Init-Pfad, dieselbe Werbe-ID, dieselben News-Inhalte. Der Kontext eines gebührenfinanzierten öffentlichen Rundfunks erhöht die Erwartung an Zurückhaltung.

Die vollständige Kette (The Complete Chain)

Schritt 1: Erstmeldung 1. Juli 2026, Embargo 29. September.

Schritt 2: Vier Nachfassungen bis 31. Juli; die SRG antwortet am 31. Juli, die Erstmeldung sei nicht auffindbar.

Schritt 3: Zustellnachweis am 15. und 18. August; die SRG erkennt ihn am 18. August nicht als Nachweis an und beantwortet keine Frage.

Schritt 4: Fristerinnerung am 3. September ohne Antwort; Embargo am 29. September erreicht; Veröffentlichung 18 Tage danach, 108 Tage nach der Erstmeldung.

Datenschutz, Artikel für Artikel (Data Protection)

Art. 5(1)(b), 6(1) und 9 DSGVO: Zweckbindung und Rechtsgrundlage der Attributions- und Reichweiten-SDKs (H1, H3).

Art. 7 DSGVO: Einwilligung vor Verarbeitung (H2).

Art. 32 DSGVO: API-Schlüssel (M1), Pinning (L1).

Art. 35 DSGVO: DSFA für News-Konsumprofile mit Art.-9-Bezug (angefragt, unbeantwortet).

Regulatorisches & rechtliches Umfeld (Regulatory)

Für EWR-Nutzer gilt die DSGVO, für Schweizer Nutzer das revidierte Schweizer DSG unter Aufsicht des EDÖB, der in Kopie informiert ist. Die SRG vertritt, dass das Vorhandensein technischer Komponenten für sich weder eine Rechtsverletzung noch die Unzulässigkeit einer Datenbearbeitung begründe. Diese Position ist als Gegenposition dokumentiert; RFI-IRFOS behauptet keine Verarbeitung über die beobachteten Fakten hinaus und kennzeichnet Laufzeitfragen als nicht gemessen.

Indicators of Compromise

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

```
Package: ch.swissinfo.android 6.8.1 (895)
SHA-256: 915a2da9fccb0ade70f8eb7e1cc02393f007476b79fe99aa8dc31af44f1606d0
Firebase: [REDACTED IN PUBLIC REPORT -- disclosed privately to SRG SSR in R1]
SDKs: Adjust, AppsFlyer, Singular, comScore, Facebook, Firebase/Crashlytics,
      Usercentrics
```

Offenlegungs-Zeitlinie (Disclosure Timeline) & Ergebnis

Datum	Ereignis
2026-07-01	Erstmeldung an datenschutz@srgssr.ch und info@srgssr.ch (BCC EDÖB, DSB, EDPS)
2026-07-06	Nachfassung 1
2026-07-17	Nachfassung 2
2026-07-23	Nachfassung 3 (DSB im CC)
2026-07-31	Nachfassung 4; Antwort SRG: Eingang bestätigt, Erstmeldung nicht auffindbar, Bitte um Zustellnachweise
2026-08-15	Zustellnachweis von RFI-IRFOS
2026-08-18	Antwort SRG: Nachweis nicht anerkannt, Befunde nicht anerkannt, Fragen unbeantwortet; Antwort RFI-IRFOS mit Zustellnachweis
2026-09-03	Fristerinnerung, keine Antwort
2026-09-29	Embargo erreicht
2026-10-17	Veröffentlichung dieses Berichts

Korrespondenzbilanz: acht Sendungen von RFI-IRFOS, zwei inhaltlich abweisende Antworten der SRG Datenschutz/Rechtsdienst, keine Beantwortung der drei Fragen, kein Bounce. Der Fall wird mit diesem Bericht geschlossen. Eine nachträgliche inhaltliche Antwort wird neben den Befunden vermerkt.

Restrisiko & Empfehlungen (Residual Risk)

Die SRG hat die Befunde nicht anerkannt und keine Behebung mitgeteilt; sie sind zum Berichtsdatum nicht als behoben dokumentiert. 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.

- Nachweisen, dass Facebook, Firebase, Adjust, AppsFlyer, Singular und comScore erst nach Einwilligung initialisiert werden (Auto-Init-Provider hinter dem CMP).
 - Notwendigkeit von drei Attributions-SDKs und der AdServices-Berechtigungen für den journalistischen Auftrag begründen oder entfernen.
 - DSFA für News-Konsumprofile mit Art.-9-Bezug erstellen.
 - Google-API-Schlüssel restringieren, 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 SWIPLUS-2026-R1-001.