



Security & Privacy Disclosure, Final Report

ORF App-Familie — 19 Android-Apps (ORF TVthek, Ö1, Ö3, SOUND, FM4, News, Sport, Fußball, Teletext, ORFit, 9 Bundesland-Radios)

Ein gemeinsamer kommerzieller Tracking-Stack über die gesamte gebührenfinanzierte App-Familie, ein geteilter extrahierbarer Firebase-Schlüssel über 14 der 19 Apps, eine Außenseiter-App ohne jede Consent-Plattform auf gesundheitsnahen Fitnessdaten, und zehn Nachrichten über 73 Tage ohne eine einzige Antwort

**ÖFFENTLICHE OFFENLEGUNG, 17. OKTOBER 2026 — EMBARGO ERREICHT AM
29. SEPTEMBER 2026, KEINE ANTWORT ERHALTEN, KEINE DER FRAGEN
BEANTWORTET**

Target	Österreichischer Rundfunk (ORF), Würzburggasse 30, 1136 Wien — gesetzlich gebührenfinanzierter öffentlich-rechtliche r Rundfunk, Controller für alle 19 Apps der Familie
Apps im Scope (19)	ORF TVthek, Ö1, Ö3, ORF SOUND, Radio FM4, ORF.at News, ORF.at Sport, Fußball, Teletext, ORFit, sowie die 9 Bundesland- Radios (Burgenland, Kärnten, Niederösterreich, Oberösterreich, Salzburg, Steiermark, Tirol, Vorarlberg, Wien)
Platform Audited	Android, statische Analyse der produktiven APKs
Initial Disclosure (R1)	2026-07-01, an datenschutz@orf.at, BCC österreichische Datenschutzbehörde (DSB) und EDPS
Disclosure / Embargo Date	2026-09-29
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	8 (1 Critical, 3 High, 3 Medium, 1 Low)
Correspondence	10 Nachrichten von RFI-IRFOS über 73 Tage (2026-07-01 bis 2026-09-12), 0 Antworten erhalten, nicht einmal eine Emp- fangsbestätigung
Authorities Notified	Österreichische Datenschutzbehörde (dsb@dsb.gv.at) · Euro- pean Data Protection Supervisor (EDPS, edps@edps.europa.e u)

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	Subject & Scope	5
3	Engagement Summary	5
4	Portfolio-Fingerprint — Alle 19 Apps im Einzelnachweis	6
5	Findings	8
5.1	C1: ORFit (com.catapult.orf): gesundheitsnahe Aktivitäts- und Sensordaten ohne erkennbare Consent-Plattform	8
5.2	H1: Voller kommerzieller Ad-Tech- und Attributions-Stack auf einem gebühren-finanzierten öffentlichen Rundfunk	9
5.3	H2: Geteilter, extrahierbarer Firebase-Schlüssel (Projekt orf-push) über 14 der 19 Apps	10
5.4	H3: Global erlaubtes Klartext-HTTP auf ORF Ö3 (alle Domains, nicht nur eigene Streaming-Hosts)	10
5.5	M1: Didomi-Consent-Plattform in 18 von 19 Apps vorhanden, Gate-Verhalten der Auto-Init-ContentProvider nicht durch statische Analyse belegbar	11
5.6	M2: ORF.at News und ORF.at Sport nutzen jeweils eigene, vom Familien-Baseline abweichende Firebase-Projekte	11
5.7	M3: Radio FM4 läuft unter einem Drittfirmen-Package-Namespace mit Zugriff auf ORFs orf-push-Firebase-Projekt	12
5.8	L1: allowBackup="true" auf mehreren Familien-Apps, eine fehlerhaft deklarierte Permission auf Fußball	12
6	Impact Analysis	12
7	The Complete Chain: Zehn Nachrichten, 73 Tage, null Antworten	13
8	Data Protection — Artikel für Artikel	13
9	Regulatory & Legal Landscape	14
10	Indicators of Compromise	14
11	Disclosure Timeline & Outcome	15
12	Residual Risk & Recommendations	15

Executive Summary

Die ORF-App-Familie umfasst 19 eigenständige Android-Apps unter der Kontrolle des Österreichischer Rundfunk (ORF), finanziert durch den verpflichtenden ORF-Beitrag. Eine statische Analyse aller 19 produktiven APKs zeigt eine gemeinsame Tracking-Infrastruktur über praktisch die gesamte Familie hinweg: die Didomi IAB-TCF Consent-Management-Plattform, INFOnline/IOMB (ÖWA-Reichweitenmessung), AppsFlyer (kommerzielles Marketing-Attribution-SDK) und Google Ad Manager/IMA (Werbeausspielung) sind in 18 der 19 Apps nachweisbar vorhanden — auf einem gebührenfinanzierten öffentlichen Rundfunk, einschließlich dessen Nachrichten- und Politik-Angeboten.

Die Familie zerfällt technisch in zwei Hauptlinien und einen Ausreißer: Eine Video-Linie (ORF TVthek, gebaut von nousguide GmbH, mit zusätzlich GfK Sentic TV-Reichweitenmessung, Google IMA und Bitmovin-Player), eine Audio/Regional-Linie (Ö1, Ö3, SOUND, Teletext, FM4, 9 Bundesland-Radios, gebaut von ORF in-house bzw. APA – Austria Presse Agentur, mit Firebase Analytics/FCM/Crashlytics auf einem einzigen geteilten Projekt 'orf-push'), und ORFit (com.catapult.orf), eine von der Drittfirma Catapult gebaute Fitness-App unter der ORF-Marke, die als einzige App der Familie ****keine erkennbare Consent-Plattform**** besitzt, während sie gleichzeitig AppsFlyer, Google AdMob, AppLovin und die Google Advertising ID ausliefert — auf Aktivitäts-, Standort- und Bluetooth-Herzfrequenzdaten (Polar-Sensor-Integration).

Der mit Abstand gravierendste Einzelbefund (C1) betrifft genau diese App: gesundheitsnahe Fitness- und Aktivitätsdaten werden ohne jede nachweisbare Consent-Gatehaltung an ein kommerzielles Tracking-/Attribution-Stack weitergegeben, und die Telemetrie läuft über ein eigenes, von Catapult kontrolliertes Firebase-Projekt statt über die ORF-eigene Infrastruktur. Zusätzlich teilen 14 der 19 Apps einen einzigen extrahierbaren Firebase-API-Schlüssel (Projekt 'orf-push') — ein Schlüssel, ein Blast-Radius über fast die gesamte Familie. ORF Ö3 erlaubt zudem global Klartext-HTTP zu allen Domains, nicht nur zu den eigenen Streaming-Hosts, womit das Hörverhalten jedes Nutzers auf dem Netzwerkpfad mitlesbar ist.

RFI-IRFOS meldete diese Befunde am 1. Juli 2026 an datenschutz@orf.at, mit der österreichischen Datenschutzbehörde und der EDPS in BCC, und nannte ein Embargo-Datum von 29. September 2026. Neun weitere Nachrichten (6., 17., 23., 31. Juli, 9., 15., 24., 31. August, 12. September 2026) wiederholten jeweils die Befunde über insgesamt 73 Tage — keine davon erhielt irgendeine Antwort, nicht einmal eine Empfangsbestätigung. Das Embargo ist nun 18 Tage überfällig, ohne dass ORF zu einem einzigen der acht Befunde Stellung genommen hätte.

ID	Severity	Title
C1	CRITICAL	ORFit (com.catapult.orf): gesundheitsnahe Aktivitäts- und Sensordaten ohne erkennbare Consent-Plattform
H1	HIGH	Voller kommerzieller Ad-Tech- und Attributions-Stack auf einem gebührenfinanzierten öffentlichen Rundfunk
H2	HIGH	Geteilter, extrahierbarer Firebase-Schlüssel (Projekt orf-push) über 14 der 19 Apps
H3	HIGH	Global erlaubtes Klartext-HTTP auf ORF Ö3 (alle Domains, nicht nur eigene Streaming-Hosts)

ID	Severity	Title
M1	MEDIUM	Didomi-Consent-Plattform in 18 von 19 Apps vorhanden, Gate-Verhalten der Auto-Init-ContentProvider nicht durch statische Analyse belegbar
M2	MEDIUM	ORF.at News und ORF.at Sport nutzen jeweils eigene, vom Familien-Baseline abweichende Firebase-Projekte
M3	MEDIUM	Radio FM4 läuft unter einem Drittfirmen-Package-Namespace mit Zugriff auf ORFs orf-push-Firebase-Projekt
L1	LOW	allowBackup="true" auf mehreren Familien-Apps, eine fehlerhaft deklarierte Permission auf Fußball

Subject & Scope

Der Österreichische Rundfunk (ORF) ist der gesetzlich gebührenfinanzierte öffentlich-rechtliche Rundfunk Österreichs; jeder Haushalt ist gesetzlich zur Finanzierung verpflichtet. Diese Offenlegung behandelt 19 Android-Apps der ORF-Familie als einen zusammenhängenden Fall, weil die zugrunde liegende Tracking-Infrastruktur über die gesamte Familie hinweg geteilt wird, auch wenn die konkreten Prozessoren unterschiedlich sind: nousguide GmbH baut ORF TVthek; ORF-interne Entwicklung und APA – Austria Presse Agentur bauen die Audio- und Regional-Apps (Ö1, Ö3, SOUND, Teletext, FM4, die 9 Bundesland-Radios, News, Sport, Fußball); und die Drittfirma Catapult baut ORFit unter der ORF-Marke. DPO-Kontakt ist datenschutz@orf.at (ORF-öffentlicher Datenschutz, nicht im Binary hartcodiert).

Engagement Summary

RFI-IRFOS sandte die vollständigen Befunde am 1. Juli 2026 an datenschutz@orf.at, mit der österreichischen Datenschutzbehörde und der EDPS in BCC, und nannte ein Embargo von 29. September 2026. Acht weitere Nachrichten folgten (6., 17., 23., 31. Juli; 9., 15., 24., 31. August 2026), wobei die Datenschutzbehörde ab der Nachricht vom 17. Juli durchgehend in sichtbarer CC stand. Eine zehnte und letzte Nachricht am 12. September 2026 — 73 Tage nach der ursprünglichen Offenlegung — fasste den vollständigen Befundstand nochmals zusammen, diesmal ohne BCC/CC, allein an datenschutz@orf.at. Über die gesamte Korrespondenz von zehn Nachrichten und 73 Tagen hinweg erhielt RFI-IRFOS ****keine einzige Antwort**** von ORF — nicht einmal eine automatische Empfangsbestätigung. Das Embargo-Datum vom 29. September 2026 ist, zum Zeitpunkt dieser Veröffentlichung, 18 Tage überfällig.

Portfolio-Fingerprint — Alle 19 Apps im Einzelnachweis

Die folgende Tabelle listet jede der 19 geprüften Apps mit Package-Namen, Firebase-Projektzuordnung, Klartext-HTTP-Status und der jeweils markantesten Abweichung vom gemeinsamen Familien-Spine (Didomi + INFOnline/IOMB + AppsFlyer + Google Ad Manager). Alle 14 Apps mit Projekt 'orf-push' teilen denselben extrahierbaren Schlüssel (Befund H2); News, Sport und ORFit laufen auf eigenen, von orf-push getrennten Firebase-Projekten (Befund M2); TVthek liefert gar kein Firebase aus.

App	Package	Firebase-Projekt	Klartext-HTTP	Markanteste Abweichung
ORF TVthek	com.nousguide.android.orftvthek	keines	global deaktiviert	GfK Sensic, Google IMA, Bitmovin; AppsFlyer+GMA+INFOnline+GAID bestätigt
Ö1	at.orf.oe1	orf-push	global (NSC erlaubt base-config)	ACCESS_COARSE_LOCATION + READ_EXTERNAL_STORAGE in reiner Audio-App
Ö3	at.orf.android.oe3	orf-push	global erlaubt, ALLE Domains	zusätzlich CAMERA, RECORD_AUDIO, ACCESS_FINE_LOCATION, WRITE_EXTERNAL_STORAGE
ORF SOUND	at.orf.sound	orf-push	erlaubt (Legacy-APA-Hosts)	ACCESS_FINE_LOCATION **und** ACCESS_COARSE_LOCATION in Audio-App; allow-Backup=true
Radio FM4	at.zuggabecke.radiofm4	orf-push	erlaubt (NSC leer, fällt auf Manifest-Default zurück)	Drittfirmen-Package-Namespace, das auf ORFs orf-push-Projekt zugreift

App	Package	Firebase-Projekt	Klartext-HTTP	Markanteste Abweichung
ORF.at News	at.orf.news	news-8d549 (eigenes, orf-push) ≠	erlaubt, keine NSC	Art.-9-Risiko: politisch-nachrichtliches Leseverhalten; allow-Backup=true
ORF.at Sport	at.orf.sport	sport-9a2eb (eigenes, orf-push) ≠	erlaubt (NSC + Manifest)	eigenes Firebase-Projekt außerhalb des orf-push-Baseline
Fußball	at.orf.sport.fussball	orf-push	erlaubt	schwerster Tracking-Stack der Familie: GfK Sensic + Bitmovin + voller Audio-Spine gleichzeitig
Teletext	at.orf.teletext	orf-push	global erlaubt + 2 zusätzliche gebündelte CA-Root-Zertifikate	Art.-9-Risiko trotz reinem Text-Dienst
ORFit	com.catapult.orf	catapult-268006 (Drittfirma, ≠ orf-push)	deaktiviert (targetSdk-36-Default)	KEINE erkennbare Consent-Plattform; Aktivitäten-/Standort-/Bluetooth-Gesundheitsdaten (siehe C1)
Radio Burgenland	at.orf.android.orfburgenland	orf-push	nur APA-Streaming-Hosts	Sentry zusätzlich zu Crashlytics (Doppel-Telemetrie)
Radio Kärnten	at.orf.android.orfkaernten	orf-push	nur APA-Streaming-Hosts	identisch zur regionalen Baseline
Radio Niederösterreich	at.orf.android.orfniederoesterreich	orf-push	nur APA-Streaming-Hosts	identisch zur regionalen Baseline
Radio Oberösterreich	at.orf.android.orfoberoesterreich	orf-push	nur APA-Streaming-Hosts	identisch zur regionalen Baseline

App		Package	Firebase-Projekt	Klartext-HTTP	Markanteste Abweichung
Radio Salzburg		at.orf.android.orfsalzburg	orf-push	nur APA-Streaming-Hosts	identisch zur regionalen Baseline
Radio Steiermark		at.orf.android.orfsteiermark	orf-push	nur APA-Streaming-Hosts	identisch zur regionalen Baseline
Radio Tirol		at.orf.android.orftirol	orf-push	nur APA-Streaming-Hosts	identisch zur regionalen Baseline
Radio Vorarlberg		at.orf.android.orfvorarlberg	orf-push	nur APA-Streaming-Hosts	identisch zur regionalen Baseline
Radio Wien		at.orf.android.orfwien	orf-push	nur APA-Streaming-Hosts	identisch zur regionalen Baseline

Findings

C1: ORFit (com.catapult.orf): gesundheitsnahe Aktivitäts- und Sensordaten ohne erkennbare Consent-Plattform

CRITICAL, 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, 9.3 — einzige App der Familie ohne jede Consent-Management-Plattform, auf gesundheitsnahen Daten

Consent-Plattform: KEINE gefunden (Didomi/OneTrust/Usercentrics/Sourcepoint/UMP alle abwesend)
Tracking/Ad-SDKs: com.appsflyer.AppsFlyerLib, com.google.android.gms.ads (AdMob), AppLovin, AdvertisingIdClient (GAID)
Sensible Permissions: ACTIVITY_RECOGNITION (Google + com.huawei.hms.permission.ACTIVITY_RECOGNITION), ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, FOREGROUND_SERVICE_LOCATION, BLUETOOTH_SCAN, BLUETOOTH_CONNECT, BLUETOOTH_ADMIN
Sensor-Integration: Polar-Herzfrequenzsensor (Bluetooth)
Firebase: eigenes Projekt catapult-268006 (Drittfirma, nicht ORFs orf-push),
Schlüssel [REDACTED IN PUBLIC REPORT -- disclosed privately to ORF in R1]

Impact: ORFit ist, von allen 19 geprüften Apps, die einzige ohne jede nachweisbare IAB-TCF- oder sonstige Consent-Management-Plattform (kein Didomi, kein OneTrust, kein Usercentrics, kein Sourcepoint, kein Google UMP) — ein kompletter Bruch mit dem sonst durchgängigen Consent-Spine der Familie. Gleichzeitig liefert die App AppsFlyer (Attribution), Google AdMob, AppLovin sowie das Auslesen der Google Advertising ID aus. Die verarbeiteten Daten sind gesundheitsnah: ACTIVITY_RECOGNITION (sowohl Google- als auch Huawei-HMS-Variante), ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, FOREG

ROUND_SERVICE_LOCATION, das vollständige Bluetooth-Cluster (SCAN/CONNECT/ADMIN) mit konkreter Polar-Herzfrequenzsensor-Integration. Die Telemetrie läuft zudem über ein eigenes, von der Drittfirma Catapult kontrolliertes Firebase-Projekt statt über ORFs eigene Infrastruktur, was die Frage nach der Verarbeiter- bzw. gemeinsamen-Verantwortlichkeits-Kette zusätzlich aufwirft. Jeder dieser Fakten ist durch statische Analyse direkt nachweisbar; es handelt sich nicht um eine Vermutung über Laufzeitverhalten.

H1: Voller kommerzieller Ad-Tech- und Attributions-Stack auf einem gebührenfinanzierten öffentlichen Rundfunk

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 7.5 — in 18 von 19 Apps bestätigt, einschließlich Nachrichten- und Sport-Angeboten

```
AppsFlyer: com.appsflyer.AppsFlyerLib, AppsFlyerRequestListener, AppsFlyerConsent
Google Ad Manager/IMA: AD_MANAGER_APP=true, googleads.g.doubleclick.net, pagead2.
googlesyndication.com
INFOOnline/IOMB: ContentProvider IOLInitProvider, config.ioam.de, de.ioam.de (auto-init
bei Prozessstart)
GfK Sentic (zusätzlich auf TVthek + Fussball): at-config.sentic.net
GAID: AdvertisingIdClient.getAdvertisingIdInfo, isLimitAdTrackingEnabled
Ausnahme: ORFit (com.catapult.orf) nutzt zwar AppsFlyer/AdMob/AppLovin, aber kein
INFOOnline/ÖWA -- siehe C1 fuer den eigenstaendigen, schwereren Befund dieser App
```

Impact: AppsFlyer (Marketing-Attribution), Google Ad Manager/IMA (Werbeausspielung inkl. Video-Ads) und mindestens ein Reichweitenmesssystem (INFOOnline/ÖWA durchgängig, zusätzlich GfK Sentic auf TVthek und Fußball) sind in 18 der 19 geprüften Apps statisch nachweisbar, einschließlich der reinen Nachrichten-App ORF.at News und der Text-Dienst-App Teletext, wo politisch relevantes Leseverhalten Art.-9-Risiken erzeugt. Die Google Advertising ID wird aktiv über AdvertisingIdClient ausgelesen. INFOOnline registriert zusätzlich einen ContentProvider (IOLInitProvider), den Android bereits beim Prozessstart instanziiert, vor jeder Consent-Anzeige — ein strukturelles Risikomuster, unabhängig davon, ob im Einzelfall tatsächlich vor einer Consent-Entscheidung übertragen wird. Ein gebührenfinanzierter öffentlicher Rundfunk, den jeder Haushalt gesetzlich mitfinanzieren muss, betreibt damit ein kommerzielles Attributions- und Werbe-Stack auf Inhalten, bei denen Art. 5(1)(a) einen erhöhten Fairness-/Transparenz-Maßstab verlangt.

H2: Geteilter, extrahierbarer Firebase-Schlüssel (Projekt orf-push) über 14 der 19 Apps

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N, 7.1 — ein Schlüssel, ein Blast-Radius über 14 Apps

```
project_id: orf-push
google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to ORF in R1]
gcm_defaultSenderId: 883710480032
per-App google_app_id variiert (z.B. 1:883710480032:android:9c59858b780d059d fuer 0e3)
, Schluessel selbst ist ueber alle 14 Apps identisch
```

Impact: Ö1, Ö3, ORF SOUND, Teletext, Radio FM4, Fußball und alle 9 Bundesland-Radios — 14 der 19 Apps — betten denselben extrahierbaren Google/Firebase-API-Schlüssel ein, verknüpft mit dem Projekt 'orf-push'. Der Wert ist in jeder dieser 14 Apps identisch; wer ihn aus einer einzigen APK extrahiert, hat ihn für alle 14. Ein ungeschützter Schlüssel dieser Art ermöglicht Kontingent- und Billing-Erschöpfung gegen das zugrunde liegende Google-Cloud-Projekt und eröffnet einen bedingten Pfad zu einem vollständigen Datenbank-Lesezugriff, falls die zugehörigen Firestore/Realtime-Database-Regeln nicht auf authentifizierten, deny-by-default-Zugriff beschränkt sind. Die Beweislast, dass diese Regeln tatsächlich gesperrt sind, liegt bei ORF/APA als Betreiber des geteilten Projekts.

H3: Global erlaubtes Klartext-HTTP auf ORF Ö3 (alle Domains, nicht nur eigene Streaming-Hosts)

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 7.1 — einzige Familien-App mit global geöffnetem Klartext-HTTP statt domänen-beschränktem

```
<base-config cleartextTrafficPermitted="true"/> -- GLOBAL, keine Domain-
Einschraenkung
Vergleich, 9 Bundesland-Radios: cleartext NUR fuer *.apa.at (mp3stream7.apasf.apa.at,
loopstream...)
Zusaetzlich in 0e3: CAMERA, RECORD_AUDIO, ACCESS_FINE_LOCATION, WRITE_EXTERNAL_STORAGE
-- ueber das regionale Set hinaus
```

Impact: ORF Ö3 (at.orf.android.oe3) deklariert in seiner Network-Security-Config ein '<base-config cleartextTrafficPermitted="true"/>' ohne Domain-Einschränkung — Klartext-HTTP ist damit zu JEDER Domain erlaubt, nicht nur zu den APA-Streaming-Hosts, wie es bei den 9 Bundesland-Radios und mehreren weiteren Familien-Apps der Fall ist (dort auf '*.apa.at' beschränkt). Das Ergebnis ist, dass das Hörverhalten jedes Ö3-Nutzers, zusammen mit jedem anderen Klartext-Request der App, auf dem Netzwerkpfad durch jeden mitlesbar ist, der sich zwischen Gerät und Server befindet — ein deutlich größerer Angriffsvektor als die bereits bei anderen Familien-Apps dokumentierte, auf Streaming-Hosts beschränkte Variante.

M1: Didomi-Consent-Plattform in 18 von 19 Apps vorhanden, Gate-Verhalten der Auto-Init-ContentProvider nicht durch statische Analyse belegbar

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.0 — Architektur vorhanden, Laufzeitverhalten reicht über statische Analyse hinaus

Impact: Eine Didomi IAB-TCF Consent-Management-Plattform mit aktuellem Vendor-Listing ist in 18 der 19 Apps vollständig gebündelt, inklusive einer expliziten AppsFlyerConsent-Verdrahtung — die Architektur ist auf Consent-Gating ausgelegt. INFOnline selbst registriert jedoch einen ContentProvider (IOLInitProvider), den Android grundsätzlich beim Prozessstart instanziiert, bevor irgendeine Activity, also auch vor jeder Consent-Anzeige, geladen wird. Ob dieser Auto-Init-Pfad in der Praxis tatsächlich Daten überträgt, bevor eine Nutzerin eine Consent-Entscheidung getroffen hat, liegt außerhalb dessen, was reine statische Codeanalyse belegen kann, und bleibt ein Gegenstand für eine dynamische Nachprüfung mit Netzwerk-Capture.

M2: ORF.at News und ORF.at Sport nutzen jeweils eigene, vom Familien-Baseline abweichende Firebase-Projekte

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 5.3 — zwei zusätzliche extrahierbare Schlüssel außerhalb des orf-push-Baseline

```
at.orf.news: project_id news-8d549, google_api_key [REDACTED IN PUBLIC REPORT --  
disclosed privately to ORF in R1]  
at.orf.sport: project_id sport-9a2eb, google_api_key [REDACTED IN PUBLIC REPORT --  
disclosed privately to ORF in R1]
```

Impact: ORF.at News führt ein eigenes Firebase-Projekt ('news-8d549'), ORF.at Sport ein eigenes ('sport-9a2eb') — beide verschieden vom geteilten 'orf-push'-Projekt des Audio/Regional-Baseline (siehe H2) und jeweils mit einem eigenen, ebenso extrahierbaren API-Schlüssel. Dies verdoppelt die Anzahl der Projekte, für die die Beweislast einer korrekten Zugriffsregel-Konfiguration getrennt getragen werden muss, und weicht ohne dokumentierten Grund vom sonst familienweit konsistenten Firebase-Modell ab.

M3: Radio FM4 läuft unter einem Drittfirmen-Package-Namespace mit Zugriff auf ORFs orf-push-Firebase-Projekt

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.6 — Verarbeiterkette für den Firebase-Zugriff nicht aus dem Package-Namespace ersichtlich

Impact: Radio FM4 wird unter dem Package-Namespace 'at.zuggabecka.radiofm4' ausgeliefert — einem Namen außerhalb jedes anderen 'at.orf.*'-Musters der Familie — nutzt dabei aber dieselbe geteilte 'orf-push'-Firebase-Infrastruktur wie der Rest der Audio/Regional-Linie. Das wirft die Frage auf, welche externe Agentur hinter diesem Namespace steht und auf welcher Art. 28-Verarbeitervereinbarung ihr Zugriff auf ORFs Firebase-Projekt beruht; aus dem Binary selbst ist diese Kette nicht ersichtlich.

L1: allowBackup="true" auf mehreren Familien-Apps, eine fehlerhaft deklarierte Permission auf Fußball

LOW, CVSS v4.0 AV:P/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.8 — gerätegebundene, nicht fernausnutzbare Härtungslücken

Impact: ORF.at News, ORF.at Sport, ORF SOUND und Radio FM4 setzen 'android:allowBackup="true"', wodurch App-private Daten über adb-Backup vom Gerät extrahierbar sind, wo ein solcher Zugriff verfügbar ist. Fußball deklariert zusätzlich eine fehlerhaft geschriebene Permission 'ANDROID.PERMISSION.READ_PHONE_STATE' (vollständig großgeschrieben, nicht die kanonische Android-Permission) — ein SDK-Artefakt, das vermutlich wirkungslos ist, aber auf eine nicht bereinigte Abhängigkeit hinweist und zur Klärung markiert wird.

Impact Analysis

Von den acht Befunden ist C1 (ORFit, fehlende Consent-Plattform auf gesundheitsnahen Daten) der einzige, der eine strukturelle Ausnahme vom sonstigen Familien-Muster darstellt, nicht dessen Fortsetzung — die anderen 18 Apps verfügen alle über eine Consent-Plattform, ORFit über keine. H1 bis H3 beschreiben Muster, die über den Großteil der Familie hinweg konsistent auftreten: ein gemeinsames kommerzielles Tracking-Stack, ein geteiltes Credential, und eine einzelne App (Ö3), die über die sonst domänenbeschränkte Klartext-Praxis der Familie hinausgeht. Keiner der acht Befunde beruht auf einer Vermutung über Laufzeitverhalten; jeder ist direkt aus dem produktiven Binary extrahiert.

The Complete Chain: Zehn Nachrichten, 73 Tage, null Antworten

Schritt 1 — Offenlegung gesendet: RFI-IRFOS sendet die vollständigen Befunde am 1. Juli 2026 an datenschutz@orf.at, mit der österreichischen Datenschutzbehörde und der EDPS in BCC, und nennt ein Embargo von 29. September 2026.

Schritt 2 — Anhaltendes Schweigen: Nachfassungen am 6. Juli (keine Antwort), 17. Juli (Datenschutzbehörde und EDPS ab hier in sichtbarer CC, keine Antwort) und 23. Juli 2026 (keine Antwort).

Schritt 3 — Weiteres Schweigen: Nachfassungen am 31. Juli, 9. August und 15. August 2026 wiederholen die Befunde erneut. Keine Antwort auf keine davon.

Schritt 4 — Fortgesetztes Schweigen: Nachfassungen am 24. August und 31. August 2026, nun 54 beziehungsweise 61 Tage seit der ursprünglichen Offenlegung. Keine Antwort.

Schritt 5 — Letzte Nachfassung: Am 12. September 2026, 73 Tage nach der ursprünglichen Offenlegung, fasst RFI-IRFOS den vollständigen Befundstand ein letztes Mal zusammen. Keine Antwort.

Schritt 6 — Embargo verstreicht unbeantwortet: Das Embargo-Datum 29. September 2026 verstreicht, ohne dass auf eine einzige der zehn Nachrichten reagiert worden wäre.

Schritt 7 — Veröffentlichung: Dieser Report erscheint 18 Tage nach dem Embargo, mit dem vollständigen, unveränderten Stand: zehn gesendete Nachrichten, null erhaltene Antworten, kein einziger der acht Befunde von ORF kommentiert.

Data Protection — Artikel für Artikel

Art. 9(1), Art. 6, Art. 7 DSGVO — Besondere Kategorien personenbezogener Daten, Rechtmäßigkeit, Einwilligung: C1s gesundheitsnahe Aktivitäts- und Sensordaten ohne jede Consent-Plattform auf ORFit stellen den schwersten Einzelbefund dieser Offenlegung dar.

Art. 5(1)(a), Art. 6(1), Art. 9 DSGVO — Fairness/Transparenz, Rechtmäßigkeit, politische Meinungsbildung: H1s familienweites Ad-Tech- und Attributions-Stack, einschließlich auf Nachrichten- und Textdienst-Apps, steht im Spannungsverhältnis zum erhöhten Maßstab, den ein gebührenfinanzierter öffentlicher Rundfunk erfüllen muss.

Art. 32(1)(b), Art. 5(1)(f) DSGVO — Sicherheit der Verarbeitung, Integrität und Vertraulichkeit: H2s geteilter Firebase-Schlüssel über 14 Apps und H3s global geöffnetes Klartext-HTTP auf Ö3 fallen hinter die von diesen Vorschriften verlangten technischen Maßnahmen zurück.

Art. 6(1), Art. 7 DSGVO — Rechtmäßigkeit und Einwilligung: M1s Auto-Init-ContentProvider-Muster bei INFOnline bleibt architektonisch ungeklärt, auch wenn eine Consent-Plattform vorhanden ist.

Art. 32(1)(b), Art. 28 DSGVO — Sicherheit der Verarbeitung, Verarbeiterverträge: M2s abweichende Firebase-Projekte auf News/Sport und M3s Drittfirmen-Package-Namespace auf FM4 werfen offene Fragen zur Verarbeiterkette auf.

Art. 32 DSGVO — Sicherheit der Verarbeitung: L1s allowBackup-Konfigurationen und die fehlerhaft deklarierte Permission auf Fußball sind geräteseitige Härtungslücken.

Regulatory & Legal Landscape

ORF ist als gesetzlich gebührenfinanzierter öffentlich-rechtlicher Rundfunk Controller für alle 19 Apps der Familie. Die österreichische Datenschutzbehörde (DSB) und die EDPS standen von Beginn der Korrespondenz an in BCC, ab der zweiten Nachfassung (17. Juli 2026) durchgehend in sichtbarer CC. Keine Antwort — weder von ORF noch indirekt über eine der Behörden — ist in den zehn Nachrichten dieser Korrespondenz dokumentiert.

Bußgeldrahmen nach DSGVO: Art. 83(4) greift für den Art.-32/Art.-5(1)(f)-Befund in H2 und H3, bis zu 10.000.000 EUR oder 2% des weltweiten Jahresumsatzes. Art. 83(5) greift für den Art.-9-Befund in C1 und den Art.-9-Aspekt in H1, bis zu 20.000.000 EUR oder 4% des weltweiten Jahresumsatzes. Vollständiges Schweigen über 73 Tage und zehn Nachrichten hinweg, bei einer Behörde in durchgehender CC, ist ein Fakt, den eine Aufsichtsbehörde bei der Bewertung der internen Bearbeitung relevant finden kann.

Indicators of Compromise

Die folgenden Befunde wurden ausschließlich durch statische Analyse der 19 produktiven APKs gewonnen. Keine ORF-Server, -Konten oder -Infrastruktur wurden angetestet. Alle hartcodierten Credential-Werte sind in diesem öffentlichen Report redigiert; die vollständigen Werte wurden ORF im ursprünglichen R1-Schreiben vollständig privat mitgeteilt.

```
C1 -- ORFit (com.catapult.orf): keine Consent-Plattform, Gesundheitsnahe Sensordaten,
    eigenes Firebase catapult-268006
H1 -- AppsFlyer + Google Ad Manager/IMA + INFOnline/GfK, bestaetigt in 18/19 Apps
H2 -- Geteilter orf-push Firebase-Schlüssel, identisch in 14/19 Apps
H3 -- 0e3: global cleartextTrafficPermitted=true, nicht domain-beschränkt
M1 -- Didomi CMP in 18/19 Apps, INFOnline IOLInitProvider Auto-Init-ContentProvider
M2 -- at.orf.news (news-8d549) + at.orf.sport (sport-9a2eb), eigene Firebase-Projekte
M3 -- at.zugabebecka.radiofm4: Drittfirmen-Namespace mit orf-push-Zugriff
L1 -- allowBackup=true (News/Sport/SOUND/FM4), malformed READ_PHONE_STATE (Fussball)
```

Disclosure Timeline & Outcome

2026-07-01 Initiale Offenlegung an datenschutz@orf.at, BCC österreichische DSB und EDPS. Embargo: 2026-09-29.

2026-07-06 Nachfassung gesendet. Keine Antwort.

2026-07-17 Nachfassung gesendet, DSB und EDPS ab hier in sichtbarer CC. Keine Antwort.

2026-07-23 Nachfassung gesendet. Keine Antwort.

2026-07-31 Nachfassung gesendet. Keine Antwort.

2026-08-09 Nachfassung gesendet. Keine Antwort.

2026-08-15 Nachfassung gesendet. Keine Antwort.

2026-08-24 Nachfassung gesendet. Keine Antwort.

2026-08-31 Nachfassung gesendet. Keine Antwort.

2026-09-12 Letzte Nachfassung gesendet, 73 Tage seit der ursprünglichen Offenlegung. Keine Antwort.

2026-09-29 Embargo-Datum erreicht und verstrichen, ohne dass auf einen der acht Befunde reagiert worden wäre.

2026-10-17 Dieser Report veröffentlicht, 18 Tage nach dem Embargo. Korrespondenz-Protokoll: zehn RFI-IRFOS-Nachrichten, null Antworten, null der acht Befunde kommentiert.

Residual Risk & Recommendations

C1 – Sofortmaßnahme: eine Consent-Management-Plattform für ORFit implementieren, bevor Aktivitäts-, Standort- oder Sensordaten an AppsFlyer/AdMob/AppLovin weitergegeben werden; die Verarbeiter-/Verantwortlichkeitsbeziehung zu Catapult inklusive dessen Firebase-Projekt dokumentieren und vertraglich fassen.

H1 – Die Notwendigkeit und Rechtsgrundlage von AppsFlyer-Attribution und Google-Ad-Manager-Werbeausspielung auf einem gebührenfinanzierten öffentlichen Rundfunk überprüfen, insbesondere auf Nachrichten- und Textdienst-Angeboten.

H2 – Den geteilten orf-push-Schlüssel auf die produktiven Signaturzertifikate aller 14 betroffenen Apps beschränken, die zugehörigen Firestore/Realtime-Database-Regeln auf deny-by-default/authentifizierten Zugriff prüfen, und den Schlüssel nach Offenlegung rotieren.

H3 – Die Network-Security-Config von Ö3 auf das domänenbeschränkte Modell der restlichen Familie (nur APA-Streaming-Hosts) zurückführen.

M1 – Mit einer dynamischen Prüfung (Netzwerk-Capture) verifizieren, ob der INFOnline-IOL InitProvider-Auto-Init-Pfad tatsächlich vor einer Consent-Entscheidung überträgt, und das Ergebnis dokumentieren.

M2 – Dokumentieren, warum News und Sport eigene Firebase-Projekte außerhalb des orf-push-Baseline führen, und deren Zugriffsregeln ebenso prüfen wie bei H2.

M3 – Die Verarbeiterkette hinter dem at.zugabecke.radiofm4-Package-Namespace und dessen Zugriff auf orf-push dokumentieren.

L1 – allowBackup auf false setzen für News, Sport, SOUND und FM4; die fehlerhaft deklarierte READ_PHONE_STATE-Permission auf Fußball bereinigen oder entfernen.

Prozedural: RFI-IRFOS bleibt jederzeit offen für eine inhaltliche Antwort zu einem oder mehreren der acht Befunde; dieser Report wird aktualisiert, sobald eine solche eintrifft.

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 stammen aus statischer Analyse der

veröffentlichten Applikationen mit öffentlich verfügbaren Werkzeugen. Keine ORF-Server, -Konten oder -Infrastruktur wurden angetestet. Die in den Befunden H2, M2 und C1 referenzierten hart-codierten Credential-Werte sind in diesem öffentlichen Report redigiert; die vollständigen Werte wurden ORF im ursprünglichen R1-Schreiben vollständig privat mitgeteilt und bleiben ORF sowie einer Aufsichtsbehörde auf Anfrage verfügbar. Technische Beweise sind unter Chain-of-Custody archiviert. Forschung durchgeführt nach ISO/IEC 29147, der Freiheit der Wissenschaft (Art. 17 StGG) und DSGVO Art. 89. REF ORF-2026-R1-001.