



---

# Security & Privacy Disclosure, Final Report

[MagellanTV \(com.abide.magellantv\)](https://com.abide.magellantv)

Firestore and Meta SDKs that initialize before any consent mechanism exists, cleartext HTTP permitted app-wide with no certificate pinning, hardcoded Firestore identifiers and player license keys, an undisclosed attribution stack and no EU representative, unresolved through 103 days and a 13-day-overdue embargo, with the only public contact address forwarding into a deleted mailbox

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 4 OCTOBER 2026, FIVE FINDINGS REMAIN UNADDRESSED**

---

|                                  |                                                                                                                                              |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target</b>                    | MagellanTV, LLC, 1875 Connecticut Ave NW, Floor 10, Washington, DC 20009, USA                                                                |
| <b>Package</b>                   | com.abide.magellantv                                                                                                                         |
| <b>Platform Audited</b>          | Android · mob.3.1.0 (versionCode 1418), static analysis of the production APK and splits                                                     |
| <b>Initial Disclosure (R1)</b>   | 2026-07-06 (REF com.abide.magellantv)                                                                                                        |
| <b>Disclosure / Embargo Date</b> | 2026-10-04                                                                                                                                   |
| <b>Report Published</b>          | 2026-10-17                                                                                                                                   |
| <b>Overall Severity</b>          | HIGH                                                                                                                                         |
| <b>Findings</b>                  | 5 (2 High, 3 Medium)                                                                                                                         |
| <b>Correspondence</b>            | 4 messages sent by RFI-IRFOS over 49 days, 2 Undeliverable notices for the forwarding target of connect@magellantv.com, no reply of any kind |
| <b>Authorities in copy</b>       | Austrian Datenschutzbehörde (DSB) - European Data Protection Supervisor (EDPS)                                                               |

---

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

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

## Contents

---

|           |                                                                                                                    |           |
|-----------|--------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b>  | <b>Executive Summary</b>                                                                                           | <b>4</b>  |
| <b>2</b>  | <b>Subject &amp; Operator Context</b>                                                                              | <b>5</b>  |
| <b>3</b>  | <b>Engagement Summary</b>                                                                                          | <b>5</b>  |
| <b>4</b>  | <b>Findings</b>                                                                                                    | <b>5</b>  |
| 4.1       | H1: Firebase and Meta SDKs initialize at process start with no consent management platform in the binary . . . . . | 5         |
| 4.2       | H2: Cleartext traffic permitted app-wide on targetSdk 35, with no certificate pinning . . . . .                    | 6         |
| 4.3       | M1: Firebase project identifiers and third-party player license keys hardcoded in the binary . . . . .             | 7         |
| 4.4       | M2: Advertising ID and attribution stack in a subscription app, not surfaced in the app . . . . .                  | 8         |
| 4.5       | M3: No Art. 27 EU representative and no data protection officer named in the controller's privacy policy . . . . . | 8         |
| <b>5</b>  | <b>Impact Analysis</b>                                                                                             | <b>9</b>  |
| <b>6</b>  | <b>The Complete Chain: From Install to Unanswered Exposure</b>                                                     | <b>9</b>  |
| <b>7</b>  | <b>Data Protection — Article by Article</b>                                                                        | <b>9</b>  |
| <b>8</b>  | <b>Regulatory &amp; Legal Landscape</b>                                                                            | <b>10</b> |
| <b>9</b>  | <b>Indicators of Compromise</b>                                                                                    | <b>10</b> |
| <b>10</b> | <b>Disclosure Timeline &amp; Outcome</b>                                                                           | <b>10</b> |
| <b>11</b> | <b>What MagellanTV Got Right</b>                                                                                   | <b>11</b> |
| <b>12</b> | <b>Residual Risk &amp; Recommendations</b>                                                                         | <b>11</b> |

## Executive Summary

MagellanTV (com.abide.magellantv, mob.3.1.0) is a documentary streaming app operated by MagellanTV, LLC of Washington, DC. A static analysis of the production APK produced five findings, two HIGH and three MEDIUM. Firebase and the Meta SDK initialize through Content-Providers at process start while the binary contains no consent management platform and no in-app consent screen (H1). The app permits cleartext HTTP to every domain on targetSdk 35 and pins no certificate (H2). Firebase identifiers and two player license keys are hard-coded (M1). An advertising ID and attribution stack is not surfaced in the app (M2), and the controller's privacy policy names neither a data protection officer nor an EU representative (M3).

The disclosure went to connect@magellantv.com on 6 July 2026, the only public contact. The follow-up of 23 July returned an Undeliverable notice from MagellanTV's own Office 365 system, which showed that connect@magellantv.com forwards to a blueantmedia.com mailbox that no longer exists. The messages of 9 and 24 August went to info@magellantv.com and raised no bounce. Four messages over 49 days produced no reply of any kind. The embargo expired on 4 October 2026 with all five findings unaddressed, and none of the three questions has been answered.

The audit also found a profile better than most of the series: no ad serving or ad mediation SDK, no session replay SDK, no automatic content recognition SDK, no Chinese or Russian SDK, a lean permission set, backups disabled, and payment handling through Google Play Billing and Amazon IAP. The five findings stand on top of that baseline.

| ID | Severity      | Title                                                                                                |
|----|---------------|------------------------------------------------------------------------------------------------------|
| H1 | <b>HIGH</b>   | Firebase and Meta SDKs initialize at process start with no consent management platform in the binary |
| H2 | <b>HIGH</b>   | Cleartext traffic permitted app-wide on targetSdk 35, with no certificate pinning                    |
| M1 | <b>MEDIUM</b> | Firebase project identifiers and third-party player license keys hardcoded in the binary             |
| M2 | <b>MEDIUM</b> | Advertising ID and attribution stack in a subscription app, not surfaced in the app                  |
| M3 | <b>MEDIUM</b> | No Art. 27 EU representative and no data protection officer named in the controller's privacy policy |

## Subject & Operator Context

---

MagellanTV, LLC operates MagellanTV, a documentary streaming service, from Washington, DC. The operator identity comes from the copyright string embedded in the app and from public corporate records. The app is a native Kotlin and Java Android application with a Bitmovin player, Widevine DRM, Firebase, Meta App Events and Google Tag Manager. With no EU establishment identified, no one-stop-shop lead authority exists, and the Austrian Datenschutzbehörde is competent for the Austrian initiated matter.

## Engagement Summary

---

RFI-IRFOS sent the initial disclosure on 6 July 2026 to connect@magellantv.com with the Austrian DSB and the EDPS in copy and fixed a 90-day embargo of 4 October 2026. The follow-up of 23 July to the same address returned an Undeliverable notice from MagellanTV's Office 365 system: connect@magellantv.com forwards to connect@blueantmedia.com, and that mailbox was not found.

On 9 August 2026 RFI-IRFOS wrote to info@magellantv.com with connect@magellantv.com in copy, which produced the same notice for connect@ and none for info@. A third follow-up on 24 August went to info@magellantv.com alone. No reply followed any of the four messages. This report publishes 13 days after the embargo.

## Findings

---

### H1: Firebase and Meta SDKs initialize at process start with no consent management platform in the binary

---

**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, 7.1 — Firebase and Meta SDKs initialize at process start with no consent management platform in the binary**

```
com.google.firebase.provider.FirebaseInitProvider    initOrder=100, directBootAware=true
com.facebook.internal.FacebookInitProvider
firebase_crashlytics_collection_enabled = true
com.facebook.sdk.ApplicationId (only Facebook SDK meta-data present)
Firebase registrars: Crashlytics, Analytics, RemoteConfig, Sessions
consent platform strings in 7 dex files + strings.xml: none
```

**Impact:** FirebaseInitProvider (initOrder 100, directBootAware true) and FacebookInitProvider are ContentProviders that run during Application creation, before any Activity can show a consent screen. firebase\_crashlytics\_collection\_enabled is explicitly set to true. Firebase Analytics, Crashlytics, Performance, Sessions and Remote Config load through the component discovery service, and Meta App Events is present. No manifest flag disables auto initialization and no AutoLogAppEventsEnabled or AutoInitEnabled flag exists for the Facebook SDK. Across all seven dex files and strings.xml there is no OneTrust, Didomi, Usercentrics,

Cookiebot, Sourcepoint or consentmanager string and no in-app consent screen, only external links to a privacy policy page at signup and purchase. The IABTCF preference keys in classes4.dex belong to a bundled Google Play Services module and come with no consent form class. Consent must precede processing under Art. 6(1) and Art. 7(1), and Art. 5(2) places the burden of showing otherwise on the controller. No ad mediation, biometric or minors specific processing rides along, which is why this finding is graded HIGH and not CRITICAL.

## H2: Cleartext traffic permitted app-wide on targetSdk 35, with no certificate pinning

**HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 7.0 — Cleartext traffic permitted app-wide on targetSdk 35, with no certificate pinning**

```
<application android:usesCleartextTraffic="true" android:networkSecurityConfig="@xml/
    network_security_config">
  <base-config cleartextTrafficPermitted="true" />
  <domain-config cleartextTrafficPermitted="true">
    <domain includeSubdomains="true">[REDACTED IN PUBLIC REPORT -- disclosed privately
      to MagellanTV in R1]</domain>
    <domain includeSubdomains="true">[REDACTED IN PUBLIC REPORT -- disclosed privately
      to MagellanTV in R1]</domain>
  </domain-config>
  no <pin-set> anywhere
```

**Impact:** The manifest sets android:usesCleartextTraffic to true and the network security config sets base-config cleartextTrafficPermitted to true. On targetSdk 35 the platform default blocks cleartext, so the app overrides the default twice and permits unencrypted HTTP to every domain it contacts. The config also names two raw AWS EC2 public DNS hostnames, which the base-config already covers, and which indicates a backend addressed by instance hostname instead of a stable domain with its own certificate. No pin-set exists for any endpoint, including the login and subscription API. The app handles account login, subscription state and viewing history, and Art. 32(1)(a) and (b) calls for encryption in transit proportionate to that risk. The control gap exists whether or not any given request travels over plain HTTP today, and which requests do is for MagellanTV to state.

**M1: Firebase project identifiers and third-party player license keys hardcoded in the binary**

**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 — Firebase project identifiers and third-party player license keys hardcoded in the binary**

```
google_api_key:      [REDACTED IN PUBLIC REPORT -- disclosed privately to
  MagellanTV in R1]
google_app_id:       [REDACTED IN PUBLIC REPORT -- disclosed privately to
  MagellanTV in R1]
project_id:          [REDACTED IN PUBLIC REPORT -- disclosed privately to
  MagellanTV in R1]
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to
  MagellanTV in R1]
google_storage_bucket: [REDACTED IN PUBLIC REPORT -- disclosed privately to
  MagellanTV in R1]
gcm_defaultSenderId: [REDACTED IN PUBLIC REPORT -- disclosed privately to
  MagellanTV in R1]
JW_LICENSE_KEY:      [REDACTED IN PUBLIC REPORT -- disclosed privately to
  MagellanTV in R1]
BITMOVIN_PLAYER_LICENSE_KEY: [REDACTED IN PUBLIC REPORT -- disclosed privately to
  MagellanTV in R1]
```

**Impact:** strings.xml carries the Firebase API key, app ID, project ID, Realtime Database URL, storage bucket and sender ID verbatim, and the manifest carries two video player license keys (JW Player and Bitmovin). Google documents Firebase API keys as identifiers and not secrets, so the exposure is one of quota abuse and rules configuration, and it calls for verification of Firebase Security Rules and Storage Rules. No JW Player class exists in any dex file while its key is declared, which points to a stale key from an earlier player integration, and Bitmovin is the active player. The player keys carry commercial impact for MagellanTV and no direct personal data exposure.

**M2: Advertising ID and attribution stack in a subscription app, not surfaced in the app**

**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 — Advertising ID and attribution stack in a subscription app, not surfaced in the app**

```
com.google.android.gms.permission.AD_ID
android.permission.ACCESS_AD_SERVICES_ATTRIBUTION
android.permission.ACCESS_AD_SERVICES_AD_ID
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
<attribution allowAllToAccess="true" />
AdvertisingIdClient, com/facebook/appevents/*, com/google/android/gms/tagmanager/*
```

**Impact:** The manifest declares AD\_ID, ACCESS\_AD\_SERVICES\_ATTRIBUTION, ACCESS\_AD\_SERVICES\_AD\_ID and the Play install referrer binding, and ga\_ad\_services\_config.xml sets allowAllToAccess to true for the Privacy Sandbox attribution API. The binary contains AdvertisingIdClient, Meta App Events and Google Tag Manager. This is an attribution stack and not an ad serving stack, since no ad rendering module is present. MagellanTV's public privacy policy describes interest based advertising, Google Analytics and social plugin sharing. None of it appears in any in-app consent or preference screen, and strings.xml holds no advertising preference or do-not-sell copy. A generic external policy link meets Art. 13 and Art. 14 only when the policy is specific and current.

**M3: No Art. 27 EU representative and no data protection officer named in the controller's privacy policy**

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 — No Art. 27 EU representative and no data protection officer named in the controller's privacy policy**

Source: MagellanTV, LLC public privacy policy at magellantv.com, fetched 2026-07-06. Distribution evidence: EEA Play Store listing and split\_config.de.apk with German localization. No DPO and no Art. 27 representative appears in the binary or in the policy.

**Impact:** The public privacy policy of MagellanTV, LLC names no data protection officer, no EU or UK representative and contains no GDPR specific rights language, as established by direct fetch on 2026-07-06. MagellanTV, LLC is a US company in Washington, DC with no EU establishment identified, and the app is distributed on an EEA Play Store listing with a full German localization split. A controller offering services to data subjects in the Union designates a representative under Art. 27 unless an Art. 27(2) exemption applies, and a documentary subscription service has no obvious exemption. This finding rests on the controller's public documentation and not on the binary.

## Impact Analysis

---

H1 and M2 describe what the app observes about viewers and when. Analytics, crash, session and attribution SDKs start before any consent mechanism can appear, in an app that holds login, subscription and viewing history. H2 describes the channel. With cleartext permitted everywhere and no pinning, protection in transit depends on each backend choosing HTTPS. M1 and M3 describe accountability: identifiers that anyone can extract, and a controller that publishes no representative for the Union.

The correspondence record is a finding about reachability. The only public contact address forwarded into a deleted mailbox and returned Undeliverable notices from the controller's own mail system, and the second address stayed silent.

## The Complete Chain: From Install to Unanswered Exposure

---

Step 1, Install: Download MagellanTV (com.abide.magellantv) from Google Play, EEA listing.

Step 2, Process start: FirebaseInitProvider and FacebookInitProvider initialize during Application creation with Crashlytics collection set to true.

Step 3, Consent: No consent platform and no consent screen exist, only an external privacy policy link.

Step 4, Network: Cleartext HTTP is permitted for every domain and no certificate is pinned.

Step 5, Attribution: The advertising ID, install referrer, Meta App Events and Tag Manager form an attribution stack that no in-app screen describes.

Step 6, Accountability: The privacy policy names no DPO and no Art. 27 representative.

Step 7, Disclosure: The only public contact forwarded into a deleted mailbox, and four messages over 49 days led to no reply.

## Data Protection — Article by Article

---

Art. 5(1)(a) and Art. 5(2) GDPR, lawfulness, transparency and accountability: H1 and M2.

Art. 6(1) and Art. 7(1) GDPR, lawfulness and consent: H1 means SDKs process before consent can exist.

Art. 13 and Art. 14 GDPR, transparency: M2 and M3 concern what a viewer is told about the attribution stack and the controller.

Art. 25 GDPR, privacy by design: H2 and M1.

Art. 27 GDPR, EU representative: M3.

Art. 32(1)(a) and (b) GDPR, security of processing: H2 for the cleartext override, M1 for hardcoded identifiers.

Art. 37 GDPR, data protection officer: M3, where applicable.

ePrivacy Art. 5(3): H1 and M2 for access to terminal equipment.

## Regulatory & Legal Landscape

MagellanTV, LLC has no identified EU main establishment, so no lead supervisory authority applies and each concerned authority is competent for its own residents. RFI-IRFOS copied the Austrian Datenschutzbehörde and the European Data Protection Supervisor on the disclosure and on every follow-up.

## Indicators of Compromise

The following identifiers were extracted from the production APK (mob.3.1.0, versionCode 1418, analyzed 2026-07-06) by static analysis only. No MagellanTV servers, accounts or infrastructure were probed.

```
base.apk SHA-256: 0f1854226f12e2b236fc0c8894f948e7889d252ef98c4f0964d830db69b4995c
split arm64 SHA-256: aad058ce506b3e8010bd4a75e73456d8d534585518f92bd1bf1a13c6bad0d217
split de SHA-256: 86992419dce89250c944fdc3721324b052e9eb333c2a9498d2bf4266849f20ca
split xxhdpi SHA-256: 8ba1b6d5381838ccadb93b263630ee27045af5cd12db35ec21e791b45956d10e
```

```
H1 FirebaseInitProvider, FacebookInitProvider,
   firebase_crashlytics_collection_enabled=true
H2 android:usesCleartextTraffic=true, base-config cleartextTrafficPermitted=true, no
   pin-set
M1 Firebase values, JW_LICENSE_KEY, BITMOVIN_PLAYER_LICENSE_KEY (all redacted)
M2 AD_ID, ACCESS_AD SERVICES_*, ga_ad_services_config.xml allowAllToAccess=true
M3 privacy policy at magellantv.com, fetched 2026-07-06
```

## Disclosure Timeline & Outcome

2026-07-06 Initial disclosure (R1, REF com.abide.magellantv) sent to connect@magellantv.com with the Austrian DSB and the EDPS in copy. Embargo fixed at 2026-10-04. No bounce on this message.

2026-07-23 First follow-up to connect@magellantv.com, 17 days after disclosure. The Office 365 system returns an Undeliverable notice (550 5.1.10): connect@magellantv.com forwards internally to connect@blueantmedia.com and that mailbox no longer exists.

2026-08-09 Second follow-up, 34 days after disclosure, now to info@magellantv.com with connect@magellantv.com in copy. The same Undeliverable notice returns for connect@. The message to info@ raises no bounce.

2026-08-24 Third follow-up to info@magellantv.com, 49 days after disclosure. No bounce and no reply.

2026-10-04 Embargo date reached. Correspondence record: four messages sent by RFI-IRFOS, two Undeliverable notices for the forwarding target of connect@magellantv.com, zero replies of any kind from any address.

2026-10-17 This report published, 13 days after the embargo and 103 days after the original disclosure.

## What MagellanTV Got Right

---

No ad serving or ad mediation SDK exists anywhere in the binary. No session replay SDK, no automatic content recognition SDK and no Chinese or Russian SDK was found. The permission set is lean, with no location, microphone, contacts, phone state or SMS, and the camera permission serves QR code device linking only. Backups are disabled. Jetpack Security classes are present for encrypted local storage. Payments run through Google Play Billing and Amazon IAP with no raw card data in the binary. targetSdk 35 is current.

These choices do not offset the findings. A lean permission set says nothing about initialization before consent, and a current targetSdk makes the explicit cleartext override more significant.

## Residual Risk & Recommendations

---

H1 — Add a consent management platform, disable Firebase and Meta auto initialization in the manifest, and start each SDK only after an affirmative choice.

H2 — Remove usesCleartextTraffic and the cleartext base-config, serve every endpoint over TLS, and add pin-sets for the login and subscription endpoints.

M1 — Restrict the Firebase API key, verify Security Rules and Storage Rules, and remove the stale JW Player key.

M2 — Surface the attribution stack in an in-app preference screen and restrict the attribution API from allowAllToAccess.

M3 — Designate an Art. 27 representative, name a contact for data protection matters and add GDPR rights language to the privacy policy.

Process — Repair the connect@magellantv.com forwarding rule and give the inbox a named owner who answers the three questions of this disclosure.

---

**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 All findings derive from static analysis of

com.abide.magellantv as published on Google Play, analyzed 2026-07-06, using publicly available tools (apktool, unzip, string extraction), and from MagellanTV's public privacy policy for M3. No MagellanTV servers, accounts or production infrastructure were probed or accessed. Technical evidence is archived under chain of custody and will be provided to the Österreichische Datenschutzbehörde on request. Research conducted under GDPR Art. 89 (scientific research exemption), ISO/IEC 29147 (coordinated disclosure standard), and the Austrian Federal Constitutional Law Art. 17 (freedom of research). REF MAGELLANTV-2026-R1.