



Security & Privacy Disclosure, Final Report

[Amazon Prime Video \(com.amazon.avod.thirdpartyclient\)](#)

Cross-service customer attribute infrastructure, Amazon ad exchange endpoints with the Advertising ID permission, microphone with Alexa voice search and fine location, and three overlapping telemetry channels in a streaming client, 108 days after disclosure and 18 days after the embargo, with one automated acknowledgment and no substantive reply

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 29
SEPTEMBER 2026, FIVE FINDINGS REMAIN UNADDRESSED**

Target	Amazon Europe Core S.à r.l. (EEA controller), Luxembourg, part of Amazon.com, Inc.
Package	com.amazon.avod.thirdpartyclient
Platform Audited	Android · v3.0.459.347, root-level code analysis of the production APK (apktool manifest and resources, 12 classes*.dex files)
Initial Disclosure (R1)	2026-07-01 (REF PRIMEVIDEO-2026-R1-001)
Disclosure / Embargo Date	2026-09-29
Report Published	2026-10-17
Overall Severity	HIGH
Findings	5 (3 High, 2 Medium)
Correspondence	8 messages sent by RFI-IRFOS over 73 days, 4 undeliverable notices from Amazon's mail system, 1 rejection from cnpd@cnpd.lu, 1 automated acknowledgment, no substantive reply
Authorities in copy	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

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	5
4.1	H1: Prime Video bundles the cross-service CustomerAttributeStore that links streaming to the unified Amazon customer record	5
4.2	H2: Amazon ad exchange endpoints and the Advertising ID permission inside a streaming client	6
4.3	H3: Microphone with Alexa voice search, fine location and phone state in one streaming app	6
4.4	M1: AWS Kinesis, Bugsnag and Firebase telemetry channels with US transfer .	7
4.5	M2: COLLECT_METRICS and DCP metrics permissions form a cross-app measurement fabric	7
5	Impact Analysis	8
6	The Complete Chain: From Install to Cross-Service Profile	8
7	Data Protection — Article by Article	9
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	9
10	Disclosure Timeline & Outcome	10
11	What Amazon Prime Video Got Right	10
12	Residual Risk & Recommendations	11

Executive Summary

The Amazon Prime Video Android client (com.amazon.avod.thirdpartyclient, v3.0.459.347) carries five findings, three HIGH and two MEDIUM, all established from the production binary. The client bundles Amazon's cross-service CustomerAttributeStore (H1), Amazon ad exchange endpoints together with the Advertising ID permission (H2), and a microphone, Alexa voice search, fine location and phone state permission set (H3). Three telemetry channels (Kinesis, Bugsnag, Firebase) and a metrics permission set complete the picture (M1, M2).

The disclosure sent on 1 July 2026 never reached a person. Amazon's mail system returned an Undeliverable notice for the first two recipient addresses because the address routes to a queue at audible.de that does not exist, and the Luxembourg CNPD address rejected the message. After four consecutive undeliverable notices RFI-IRFOS moved to privacy@amazon.com and eu-privacy@amazon.de on 12 August 2026. The only incoming message since then is one automated acknowledgment on 31 August 2026. No substantive reply arrived, and none of the three questions has been answered.

The audit also found things done well: allowBackup is disabled, cleartext traffic is blocked with a Network Security Config, the binary holds no screen capture code, no third-party advertising or session replay SDK, and no Chinese SDK. The five findings stand on top of that baseline.

ID	Severity	Title
H1	HIGH	Prime Video bundles the cross-service CustomerAttributeStore that links streaming to the unified Amazon customer record
H2	HIGH	Amazon ad exchange endpoints and the Advertising ID permission inside a streaming client
H3	HIGH	Microphone with Alexa voice search, fine location and phone state in one streaming app
M1	MEDIUM	AWS Kinesis, Bugsnag and Firebase telemetry channels with US transfer
M2	MEDIUM	COLLECT_METRICS and DCP metrics permissions form a cross-app measurement fabric

Subject & Operator Context

Amazon Prime Video is a streaming client published by Amazon with Amazon Europe Core S.à r.l. as the EEA controller. The Luxembourg CNPD is the lead supervisory authority under the one-stop-shop mechanism. The client sits next to Amazon Music, Amazon Business and Amazon Shopping in the same Amazon app family, which RFI-IRFOS audited in the same series and which share the identity layer documented in H1.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 1 July 2026 to privacy-eu@amazon.com and eu-dpo@amazon.com, with the Austrian DSB, the EDPS and cnpd@cnpd.lu in copy, and fixed a 90-day embargo of 29 September 2026. cnpd@cnpd.lu rejected the message, and Amazon's mail system answered with an Undeliverable notice because the address routes to a non-existent queue at audible.de. Follow-ups on 6 July, 17 July, 27 July and 5 August 2026 went to the same addresses and produced the same notice on every one except 6 July.

On 12 August 2026 RFI-IRFOS moved to privacy@amazon.com and eu-privacy@amazon.de with vrp-researchers@amazon.com and press@amazon.com in copy. No bounce followed. On 31 August 2026 one automated acknowledgment arrived from accountclosurerequest@amazon.de stating that Amazon is looking into the privacy query and will write back. The last follow-up on 12 September 2026 restated the three questions. No person at Amazon has replied. This report publishes 18 days after the embargo.

Findings

H1: Prime Video bundles the cross-service CustomerAttributeStore that links streaming to the unified Amazon customer record

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 — Prime Video bundles the cross-service CustomerAttributeStore that links streaming to the unified Amazon customer record

```
uses-permission: com.amazon.dcp.sso.permission.CUSTOMER_ATTRIBUTE_SERVICE
com/amazon/identity/auth/device/api/CustomerAttributeStore
com/amazon/identity/auth/device/api/CustomerAttributeKeys
attribute keys: COR, PFM, marketplace, customer_attribute
```

Impact: The manifest declares `com.amazon.dcp.sso.permission.CUSTOMER_ATTRIBUTE_SERVICE` and the binary bundles `com/amazon/identity/auth/device/api/CustomerAttributeStore` and `CustomerAttributeKeys` with the keys COR, PFM and marketplace. This is the same mechanism RFI-IRFOS documented in Amazon Music and Amazon Business. It reads Amazon account attributes shared across all Amazon apps on a device through single sign-on and places a streaming client inside the unified Amazon customer record. Linking viewing behavior to commerce and advertising profiles is a purpose limitation and transparency question under Art. 5(1)(b) and Art. 13(1)(c). The presence of the capability is a binary fact. Which

attributes are read at runtime and where they flow is for Amazon to state under Art. 5(2) accountability.

H2: Amazon ad exchange endpoints and the Advertising ID permission inside a streaming client

HIGH, 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, 7.0 — Amazon ad exchange endpoints and the Advertising ID permission inside a streaming client

```
amazon-adsystem.com
aax-us-east.amazon-adsystem.com
aax, /aps/
com.google.android.gms.permission.AD_ID
```

Impact: The binary contains amazon-adsystem.com, aax-us-east.amazon-adsystem.com, aax and /aps/ strings, and the manifest declares com.google.android.gms.permission.AD_ID. aax is Amazon's advertising exchange request path. Ad exchange endpoints together with the Advertising ID permission establish ad serving and ad measurement capability in a subscription streaming client. Whether the Advertising ID is read and ad requests fire only after an explicit Art. 7 consent is for Amazon to document under Art. 5(2). No consent evidence is visible in the client binary.

H3: Microphone with Alexa voice search, fine location and phone state in one streaming app

HIGH, 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, 7.0 — Microphone with Alexa voice search, fine location and phone state in one streaming app

```
RECORD_AUDIO, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION
READ_PHONE_STATE, GET_ACCOUNTS, BLUETOOTH
amazon.speech.permission.SEND_ALEXA_DIRECTIVE
AlexaDirective, SpeechRecognizer, voice_search, whisper, whisperplay, whispercache
```

Impact: The manifest declares RECORD_AUDIO, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, READ_PHONE_STATE, GET_ACCOUNTS and amazon.speech.permission.SEND_ALEXA_DIRECTIVE. The binary contains AlexaDirective, SpeechRecognizer, voice_search, whisper, whisperplay and whispercache classes. Voice search routes audio to Amazon speech services. A microphone, fine location and a device identifier together form a broad collection surface for a video player, and voice audio can carry biometric information that engages Art. 9. A data protection impact assessment covering this combination under Art. 35 is for Amazon to point to. Capture is user-triggered, the capability is a binary fact.

M1: AWS Kinesis, Bugsnag and Firebase telemetry channels with US transfer

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 — AWS Kinesis, Bugsnag and Firebase telemetry channels with US transfer

```
kinesis.<region>.amazonaws.com (AWS SDK Kinesis client)
com.google.firebase.provider.FirebaseInitProvider
com.bugsnag.android.performance (manifest provider)
```

Impact: The binary contains Kinesis telemetry code, the manifest registers com.google.firebase.provider.FirebaseInitProvider and a com.bugsnag.android.performance provider. Kinesis is real-time event ingestion, Bugsnag handles crash and performance data and Firebase is present. Three overlapping telemetry channels with onward US transfer call for a transparent Art. 13 description and an Art. 44 transfer basis. The AWS region table inside the bundled SDK is the standard SDK list and is not treated as evidence of any specific region in use.

M2: COLLECT_METRICS and DCP metrics permissions form a cross-app measurement fabric

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 — COLLECT_METRICS and DCP metrics permissions form a cross-app measurement fabric

```
amazon.permission.COLLECT_METRICS
com.amazon.dcp.metrics.permission.METRICS_PERMISSION
amazon.permission.USE_TCOMM
```

Impact: The manifest declares amazon.permission.COLLECT_METRICS, com.amazon.dcp.metrics.permission.METRICS_PERMISSION and amazon.permission.USE_TCOMM. These are device platform metrics permissions and part of Amazon's cross-app measurement fabric. Their scope and consent handling belong in the Art. 13 information a viewer receives.

Impact Analysis

H1 through H3 describe one pattern. A video player that holds the cross-service identity attribute store, the ad exchange path with the Advertising ID permission, and a microphone with fine location and phone state sits across the line between a streaming service and the unified Amazon commerce and advertising profile. Each element has a defensible product purpose on its own. The combination needs a documented Art. 6 basis, a consent gate before ad related processing, and an Art. 35 assessment, and none of these is visible to a viewer. M1 and M2 add three telemetry channels and a metrics permission set whose scope Art. 13 requires Amazon to describe.

The correspondence record is itself a finding about reachability. A privacy address that routes into a non-existent queue returned four undeliverable notices over five weeks, while the published disclosure channel for an EEA controller was unreachable.

The Complete Chain: From Install to Cross-Service Profile

Step 1, Install: Download Amazon Prime Video (com.amazon.avod.thirdpartyclient) from Google Play.

Step 2, Extract and decompile: Pull the production APK (v3.0.459.347) and run apktool. The manifest permissions and the class names listed in the Indicators section are present in plain-text.

Step 3, Identity: The client holds CUSTOMER_ATTRIBUTE_SERVICE and the CustomerAttributeStore classes, which read the account attributes COR, PFM and marketplace shared across Amazon apps on the device.

Step 4, Advertising: The client holds the Advertising ID permission and the aax and amazon-adsystem endpoints.

Step 5, Sensors: The client holds RECORD_AUDIO, fine and coarse location and READ_PHONE_STATE together with the Alexa voice search classes.

Step 6, Telemetry: Kinesis, Bugsnag, Firebase and the Amazon metrics permissions form the reporting layer.

Data Protection — Article by Article

Art. 5(1)(b) GDPR, purpose limitation: H1 places a streaming client inside the unified customer record.

Art. 5(1)(c) GDPR, data minimisation: H3 combines microphone, fine location and phone state in a video player, and M1 and M2 add overlapping telemetry.

Art. 6(1) and Art. 7 GDPR, lawfulness and consent: H1 and H2 call for a documented legal basis and a consent gate before Advertising ID and ad exchange processing.

Art. 9 GDPR, special categories: H3 voice audio can carry biometric information.

Art. 13 GDPR, transparency: H1, M1 and M2 call for a description of recipients and purposes.

Art. 35 GDPR, impact assessment: H3 calls for an assessment covering microphone, location and device identifier together.

Art. 44 GDPR, transfers: M1 sends telemetry to US infrastructure.

Regulatory & Legal Landscape

The Luxembourg CNPD is the lead supervisory authority for Amazon Europe Core S.à r.l. RFI-IRFOS copied cnpd@cnpd.lu on the original disclosure and the address rejected the message. The Austrian Datenschutzbehörde and the European Data Protection Supervisor were copied on the disclosure and on follow-ups from 5 August 2026. The EEA one-stop-shop identification in this report is an inference from Amazon's EU seat.

Indicators of Compromise

The following identifiers were extracted from the production APK (v3.0.459.347, base.apk SHA-256 1fa9d38008d066f651f0cc1e8edc1235c580cd8c0685970a0afa91f9de82fe71, analyzed 2026-07-01) by static analysis only. No Amazon servers, accounts or infrastructure were probed.

```
H1  com.amazon.dcp.sso.permission.CUSTOMER_ATTRIBUTE_SERVICE
    CustomerAttributeStore, CustomerAttributeKeys (COR, PFM, marketplace)
H2  amazon-adsystem.com, aax-us-east.amazon-adsystem.com, aax, /aps/
    com.google.android.gms.permission.AD_ID
H3  RECORD_AUDIO, ACCESS_FINE_LOCATION, READ_PHONE_STATE
    AlexaDirective, SpeechRecognizer, whisper, whisperplay, whispercache
M1  Kinesis client, FirebaseInitProvider, com.bugsnap.android.performance
M2  amazon.permission.COLLECT_METRICS, METRICS_PERMISSION, USE_TCOMM
```

Disclosure Timeline & Outcome

2026-07-01 Initial disclosure (R1, REF PRIMEVIDEO-2026-R1-001) sent to privacy-eu@amazon.com and eu-dpo@amazon.com with the Austrian DSB, the EDPS and cnpd@cnpd.lu in copy. Embargo fixed at 2026-09-29. cnpd@cnpd.lu rejects the message as address not found. Amazon's mail system returns an Undeliverable notice because the address routes to a non-existent queue at audible.de.

2026-07-06 Follow-up to the same two addresses. No reply.

2026-07-17 Follow-up to the same two addresses, 16 days after disclosure. Undeliverable notice again.

2026-07-27 Follow-up, three questions repeated. Undeliverable notice again.

2026-08-05 Follow-up with the Austrian DSB and the EDPS in copy, 35 days after disclosure. Undeliverable notice again.

2026-08-12 Address pivot to privacy@amazon.com and eu-privacy@amazon.de, with vrp-researchers@amazon.com and press@amazon.com in copy, after four consecutive undeliverable notices. No bounce followed.

2026-08-31 Follow-up to the new addresses. Amazon's system sends one automated acknowledgment the same day from accountclosurerequest@amazon.de: "We've received and are looking into your privacy query. We'll write back shortly." No further message followed.

2026-09-12 Last follow-up, 73 days after disclosure, three weeks after the working mailbox began receiving mail. No substantive reply.

2026-09-29 Embargo date reached. Correspondence record: eight messages sent by RFI-IRFOS, four undeliverable notices from Amazon's mail system, one rejection from cnpd@cnpd.lu, one automated acknowledgment, no substantive reply from any person.

2026-10-17 This report published, 18 days after the embargo and 108 days after the original disclosure.

What Amazon Prime Video Got Right

allowBackup is false. Cleartext traffic is disabled and a Network Security Config is present. The binary holds no MediaProjection or DETECT_SCREEN_CAPTURE code, no third-party advertising network or session replay library beyond Amazon's own stack, and no Chinese SDK (the only cn-north-1 hit is the standard AWS SDK region table). A single controller with an identifiable EEA lead authority makes accountability simple to assign.

These choices do not offset the findings. Good transport and backup hygiene says nothing about the legal basis for the identity linkage, the consent gate for the ad path, or the assessment for the sensor combination.

Residual Risk & Recommendations

H1 — Document the Art. 6 basis and the purpose separation between streaming and the unified customer record, and describe the CustomerAttributeStore use in the Art. 13 information.

H2 — Place the Advertising ID read and every aax and amazon-adsystem call behind an explicit Art. 7 consent and document it.

H3 — Complete an Art. 35 assessment for microphone, fine location and phone state, and state how voice audio is handled under Art. 9.

M1 and M2 — Describe the Kinesis, Bugsnag, Firebase and metrics channels, their recipients and the Art. 44 transfer basis.

Process — Repair the privacy-eu@amazon.com routing that points to a non-existent audible.de queue, and give the privacy mailbox a named human 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.amazon.avod.thirdpartyclient as published on Google Play, analyzed 2026-07-01, using publicly available tools (apktool, dex string analysis). No Amazon servers, accounts or production infrastructure were probed or accessed. Technical evidence is archived under chain of custody and will be provided to the Commission nationale pour la protection des données 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 PRIMEVIDEO-2026-R1.