



---

# Security & Privacy Disclosure, Final Report

## ARD Mediathek Android (de.swr.avp.ard)

A hardcoded Firebase API key and a production database URL ship inside a public-broadcaster app with tens of millions of installs, Firebase Auth initializes before any consent screen and transfers to Google infrastructure in the US with no documented Art. 44-49 safeguard, and after three follow-ups a single reply arrived stating a renewed review found no indications of a violation, without ever answering any of three specific yes/no questions asked three times

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28 SEPTEMBER 2026, ONE REPLY RECEIVED, THREE SPECIFIC QUESTIONS NEVER ANSWERED**

---

|                                  |                                                                                                                                                                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target</b>                    | Suedwestrundfunk (SWR), production lead for the ARD Mediathek Android app, on behalf of the ARD alliance                                                                                                                          |
| <b>Package</b>                   | de.swr.avp.ard                                                                                                                                                                                                                    |
| <b>Platform Audited</b>          | Android, static analysis of the production APK                                                                                                                                                                                    |
| <b>Initial Disclosure (R1)</b>   | 2026-06-30, to datenschutz@swr.de, CC presse@ard.de, presse@swr.de, LfDI Baden-Wuerttemberg, EDPS                                                                                                                                 |
| <b>Disclosure / Embargo Date</b> | 2026-09-28                                                                                                                                                                                                                        |
| <b>Report Published</b>          | 2026-10-17                                                                                                                                                                                                                        |
| <b>Overall Severity</b>          | CRITICAL                                                                                                                                                                                                                          |
| <b>Findings</b>                  | 2 (1 Critical, 1 High)                                                                                                                                                                                                            |
| <b>Correspondence</b>            | 6 messages sent by RFI-IRFOS across three Gmail thread IDs (threading split by subject-line changes), 1 reply received (2026-09-08, general denial, does not address any of three specific technical questions asked three times) |
| <b>Authorities CC'd</b>          | LfDI Baden-Wuerttemberg (lead supervisory authority for SWR, poststelle@lfdi.bwl.de) · European Data Protection Supervisor (EDPS, edps@edps.europa.eu)                                                                            |

---

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       | C1: Hardcoded Firebase API key and production database URL shipped inside the production binary . . . . .                                           | 6        |
| 4.2       | H1: Firebase Auth initializes before any consent screen and transfers to Google US infrastructure with no documented Art. 44-49 safeguard . . . . . | 6        |
| <b>5</b>  | <b>Impact Analysis</b>                                                                                                                              | <b>7</b> |
| <b>6</b>  | <b>The Complete Chain: Four Months, Six Messages, One Reply, Zero Answers</b>                                                                       | <b>7</b> |
| <b>7</b>  | <b>Data Protection – Article by Article</b>                                                                                                         | <b>8</b> |
| <b>8</b>  | <b>Regulatory &amp; Legal Landscape</b>                                                                                                             | <b>8</b> |
| <b>9</b>  | <b>Indicators of Compromise</b>                                                                                                                     | <b>8</b> |
| <b>10</b> | <b>Disclosure Timeline &amp; Outcome</b>                                                                                                            | <b>9</b> |
| <b>11</b> | <b>Residual Risk &amp; Recommendations</b>                                                                                                          | <b>9</b> |

## Executive Summary

The ARD Mediathek Android app is produced and operated by Suedwestrundfunk (SWR) on behalf of the ARD alliance of German public broadcasters, with tens of millions of installs across Germany and Austria. A static analysis of the production APK found two findings, one CRITICAL and one HIGH.

The app ships a hardcoded Firebase API key together with a production database URL directly inside the binary, reachable by anyone who decompiles the app (C1). Separately, Firebase Auth initializes automatically before any consent screen can render, and the resulting authentication and device data is transferred to Google's US infrastructure with no documented Art. 44-49 transfer safeguard identified in the app's privacy information (H1).

RFI-IRFOS disclosed these findings on 30 June 2026 to datenschutz@swr.de, CC presse@ard.de, presse@swr.de, the LfDI Baden-Wuerttemberg, and the European Data Protection Supervisor, stating an embargo date of 28 September 2026. Four follow-ups were sent (17 July, 27 July, 9 August, 29 August 2026), each restating the two findings and three specific yes/no technical questions, none of which drew a reply. On 8 September 2026, mediathek@ard.de replied, the first and only reply received across the entire correspondence, stating that 'a renewed review found no indications of a violation,' without addressing a single one of the three specific questions asked. RFI-IRFOS responded the same day with a six-point rebuttal, restated the three questions a third time, and set an interim deadline of 15 September 2026 for direct answers to those three questions specifically, separate from the main embargo. That interim deadline passed with no further reply, and the main embargo of 28 September 2026 has now also passed, 19 days overdue, with all three questions still unanswered on the day this report publishes.

| ID | Severity        | Title                                                                                                                                 |
|----|-----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| C1 | <b>CRITICAL</b> | Hardcoded Firebase API key and production database URL shipped inside the production binary                                           |
| H1 | <b>HIGH</b>     | Firebase Auth initializes before any consent screen and transfers to Google US infrastructure with no documented Art. 44-49 safeguard |

## Subject & Operator Context

---

Suedwestrundfunk (SWR) is one of the nine regional public-broadcasting institutions that make up the ARD alliance in Germany, and is the production lead for the ARD Mediathek app, the alliance's shared video-on-demand platform. As an Anstalt des oeffentlichen Rechts (public-law institution), SWR falls under the supervision of the LfDI Baden-Wuerttemberg, the lead authority cc'd throughout this correspondence.

## Engagement Summary

---

RFI-IRFOS sent the initial disclosure on 30 June 2026 to [datenschutz@swr.de](mailto:datenschutz@swr.de), [CCpresse@ard.de](mailto:CCpresse@ard.de), [presse@swr.de](mailto:presse@swr.de), the LfDI Baden-Wuerttemberg, and the EDPS, stating an embargo date of 28 September 2026. Follow-ups were sent on 17 July and 27 July 2026 (first thread), then 9 August and 29 August 2026 (a second thread, after Gmail's threading split on a subject-line change), each restating the two findings and three specific technical yes/no questions: whether the hardcoded key had been rotated, whether the exposed database URL had been access-restricted, and whether the Firebase Auth pre-consent initialization had been gated behind the app's consent flow.

On 8 September 2026, in a third thread, [mediathek@ard.de](mailto:mediathek@ard.de) replied for the first and only time in the entire correspondence, with a general statement that 'a renewed review found no indications of a violation of data protection requirements,' thanking RFI-IRFOS for the analysis but not engaging with any of the three specific questions. RFI-IRFOS replied the same day, within roughly 80 minutes, with a six-point rebuttal explaining precisely why a general denial does not answer a specific technical question, restated all three questions verbatim a third time, and set an interim deadline of 15 September 2026 for direct answers to those three questions, independent of the main embargo. No further reply arrived after 8 September 2026. The interim deadline passed unaddressed, and the main embargo, now 19 days overdue, has passed the same way.

## Findings

---

## C1: Hardcoded Firebase API key and production database URL shipped inside the production binary

**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, 8.2) — reachable by anyone who decompiles a tens-of-millions-install public-broadcaster app**

Firebase API key: hardcoded in resources, extractable via static decompilation  
Production database URL: hardcoded alongside the key  
Reachable by: any party decompiling the published APK

**Impact:** The production APK ships a hardcoded Firebase API key alongside a production database URL, both directly extractable via static decompilation with no additional tooling. Any party who decompiles the app, a routine step for any researcher or attacker, obtains both the key and the exact endpoint it authenticates against. For an app with tens of millions of installs operated by a public broadcaster, this is a direct violation of the technical-measures requirements of Art. 32 and the integrity-and-confidentiality principle of Art. 5(1)(f).

## H1: Firebase Auth initializes before any consent screen and transfers to Google US infrastructure with no documented Art. 44-49 safeguard

**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, 5.3) — authentication and device data transferred internationally before the user has made any choice**

FirebaseInitProvider: auto-init at process start, before consent screen render  
Authentication + device metadata destination: Google infrastructure, United States  
Documented Art. 44-49 safeguard for this flow: none identified

**Impact:** Firebase Auth initializes automatically at app start, via Firebase's standard Content-Provider auto-init mechanism, before any consent screen can render. The resulting authentication session and device metadata are transferred to Google's US infrastructure. No documented Art. 44-49 transfer safeguard (adequacy decision, Standard Contractual Clause, or equivalent) for this specific flow was identified anywhere in the app's available privacy information, and the transfer itself begins before the user has made any consent choice.

## Impact Analysis

---

C1 and H1 are both routine, fixable engineering gaps rather than deliberate design choices, the kind this disclosure series sees regularly. What sets this case apart procedurally is the single reply that did arrive: a general statement that a renewed review found no indications of a violation, sent without engaging with either finding's underlying technical question. A denial that does not name which fact it disputes is not a rebuttal, it is a restatement of the original position with no new information, and RFI-IRFOS's six-point same-day response said exactly that, in writing, before the interim deadline it set was itself allowed to pass unanswered.

## The Complete Chain: Four Months, Six Messages, One Reply, Zero Answers

---

Step 1 – Disclosure sent: RFI-IRFOS sends the full findings on 30 June 2026 to datenschutz@swr.de, CC presse@ard.de, presse@swr.de, the LfDI Baden-Wuerttemberg, and the EDPS, stating an embargo of 28 September 2026.

Step 2 – First silence: Follow-ups on 17 July and 27 July 2026 restate both findings and the three specific questions. No reply.

Step 3 – Thread split, continued silence: After a subject-line change splits the Gmail thread, further follow-ups on 9 August and 29 August 2026 restate the same findings and questions again. No reply.

Step 4 – The one reply: On 8 September 2026, in a third thread, mediathek@ard.de replies for the first time in the entire record, stating that a renewed review found no indications of a violation. None of the three specific questions is addressed.

Step 5 – Same-day rebuttal and interim deadline: RFI-IRFOS replies within roughly 80 minutes with a six-point explanation of why a general denial does not answer a specific technical question, restates all three questions a third time, and sets an interim deadline of 15 September 2026 for direct answers to those three questions specifically.

Step 6 – Interim deadline passes unanswered: 15 September 2026 passes with no further reply of any kind.

Step 7 – Main embargo reached and passed: 28 September 2026, the original embargo date, passes the same way. It is now 19 days overdue.

Step 8 – Publication: This report publishes with the full record intact: six messages sent, one reply received, and that one reply did not answer a single one of the three questions asked three times.

## Data Protection – Article by Article

---

Art. 32(1)(b), Art. 5(1)(f) GDPR – Security of processing, integrity and confidentiality: C1's hardcoded Firebase key and production database URL fall short of the technical measures these provisions require.

Art. 44 GDPR – General principle for transfers: H1's Firebase Auth data flow to Google US infrastructure has no documented safeguard for this specific flow.

Art. 6, Art. 7 GDPR – Lawfulness of processing and conditions for consent: H1's pre-consent Firebase Auth initialization begins the transfer before any consent interaction with the user.

## Regulatory & Legal Landscape

---

As an Anstalt des oeffentlichen Rechts, SWR is supervised by the LfDI Baden-Wuerttemberg, cc'd on this correspondence from the first message onward. The EDPS was also cc'd given the ARD Mediathek app's distribution across the EU, and the Austrian DSB given RFI-IRFOS's Austrian registration and the app's availability in Austria.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32 and Art. 5(1)(f) security-and-confidentiality issue in C1, up to EUR 10,000,000 or 2% of total worldwide annual turnover (for public-law broadcasters, the applicable sanction regime may run through the respective state media law rather than a turnover-based fine, a question for the supervisory authority to resolve). Art. 83(5) applies to the Art. 44, 6, and 7 issues in H1, up to EUR 20,000,000 or 4% of total worldwide annual turnover under the general regime. The single reply received, which asserted a conclusion without addressing the specific facts in dispute, is itself a fact a regulator may find relevant to how seriously the initial disclosure was actually reviewed.

## Indicators of Compromise

---

The following identifiers were extracted from the production APK via static analysis only. No SWR or ARD servers, accounts, or infrastructure were probed.

```
C1 -- Hardcoded Firebase API key + production database URL,  
    extractable via static decompilation
```

```
H1 -- FirebaseInitProvider, auto-init pre-consent,  
    transfer destination: Google infrastructure, United States
```

## Disclosure Timeline & Outcome

---

2026-06-30 Initial disclosure sent to datenschutz@swr.de, CC presse@ard.de, presse@swr.de, LfDI Baden-Wuerttemberg, EDPS. Embargo stated as 2026-09-28.

2026-07-17 Follow-up sent. No reply.

2026-07-27 Follow-up sent. No reply.

2026-08-09 Follow-up sent (new thread after subject-line change). No reply.

2026-08-29 Follow-up sent. No reply.

2026-09-08 mediathek@ard.de replies for the first and only time: a renewed review found no indications of a violation, no specific question addressed. RFI-IRFOS replies the same day, roughly 80 minutes later, with a six-point rebuttal and an interim deadline of 2026-09-15 for direct answers to three specific questions.

2026-09-15 Interim deadline passes. No further reply.

2026-09-28 Main embargo date reached and passed. Correspondence record: six RFI-IRFOS messages, one reply received, zero of three questions answered.

2026-10-17 This report published, 19 days after the embargo date.

## Residual Risk & Recommendations

---

C1 – Immediate: rotate the hardcoded Firebase API key, remove the production database URL from the binary, and restrict database access rules server-side rather than relying on client-side secrecy.

H1 – Immediate: gate Firebase Auth initialization behind the app's consent flow, and document an Art. 44-49 safeguard for the resulting authentication and device-metadata transfer to Google's US infrastructure.

Procedural: a reply asserting that a review found no violation, without engaging with the specific technical questions that prompted the disclosure, does not resolve either finding. RFI-IRFOS remains open to a substantive answer to the three questions on record at any time; this report will be updated to reflect one if it arrives.

---

**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 the published application using publicly available tooling. No SWR or ARD servers, accounts, or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF ARD-MEDIATHEK-2026.