



Security & Privacy Disclosure, Final Report

ZDF Mediathek Android (com.zdf.android.mediathek)

An advertising identifier and a commercial attribution SDK inside a fee-funded, advertising-free public-service app, one reply that disputed the assessments and named a legal basis for usage measurement, and no answer to the specific questions asked

PUBLIC DISCLOSURE, 17 OCTOBER 2026 - EMBARGO REACHED 28 SEPTEMBER 2026, EIGHT MESSAGES SENT, ONE REPLY ON 10 JULY, NO REPLY TO ANY FOLLOW-UP

Target	Zweites Deutsches Fernsehen (ZDF), Mainz. Privacy contact: datenschutz@zdf.de
Package	com.zdf.android.mediathek (APK 20.7 MB, 18,328 smali classes)
Platform Audited	Android, static analysis of the production APK, analysis date 2026-06-30
Initial Disclosure (R1)	2026-06-30, to datenschutz@zdf.de and kommunikation@zdf.de, CC presse@zdf.de, Austrian Datenschutzbehoerde, CERT.at, EDPS and LfDI Rheinland-Pfalz
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	HIGH
Findings	4 (2 High, 2 Medium, 0 Critical). The original disclosure listed 1 Critical and 3 High; see the re-scoring note in the Engagement Summary
Correspondence	8 messages sent by RFI-IRFOS over 74 days (2026-06-30 to 2026-09-12). 1 reply received (2026-07-10, from ZDF's data protection officer). 3 delivery failures: kommunikation@zdf.de twice, edps@europa.eu once. No reply to any of the 5 follow-ups after the 10 July reply
Authorities Notified	Austrian Datenschutzbehoerde (dsb@dsb.gv.at) · CERT.at (cert@cert.at) · European Data Protection Supervisor (EDPS, edps@edps.europa.eu) · LfDI Rheinland-Pfalz (poststelle@lfdi.rlp.de)

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	6
4.1	H1: Hardcoded Firebase/Google API key and production Realtime Database URL in the app resources	6
4.2	H2: Advertising identifier (AD_ID) declared by a fee-funded app that is advertising-free by statute	7
4.3	M1: Adjust attribution SDK embedded in a public-service app	7
4.4	M2: Firebase initialisation before the consent screen, with Firebase Authentication and Firestore integrated	8
5	Impact Analysis	8
6	The Complete Chain: Eight Messages, 74 Days, One Reply, Five Follow-ups Unanswered	9
7	Data Protection – Article by Article	9
8	Regulatory & Legal Landscape	10
9	Indicators of Compromise	10
10	Disclosure Timeline & Outcome	10
11	Residual Risk & Recommendations	11

Executive Summary

The ZDF Mediathek app is the Android client of Germany's public-service broadcaster ZDF, financed by the Rundfunkbeitrag. Static analysis of the production APK found four findings: one HIGH for a hardcoded Firebase/Google API key and the production Realtime Database URL, one HIGH for the declared Google advertising identifier (AD_ID) in an app that is advertising-free by statute, and two MEDIUM for an embedded Adjust attribution SDK and for Firebase initialisation before the consent screen, with Firebase Authentication and Firestore integrated.

ZDF's data protection officer replied once, on 10 July 2026. The reply records that the notes were assessed, expressly does not share RFI-IRFOS's assessments and legal conclusions, names Art. 6(1)(e) GDPR with the statutory duties of the Medienstaatsvertrag as the basis for usage measurement, states that the presence of a Firebase key, a permission or an SDK does not by itself establish a vulnerability or processing, states that LfDI Rheinland-Pfalz has no jurisdiction over ZDF, declines paid services, and declines to give information on internal architecture, security measures and contracts. This report records those positions as given.

The reply does not say why the advertising identifier specifically is declared, whether broadcasting-contribution funds pay for install campaigns measured through Adjust, which transfer mechanism covers Firebase, or which key restrictions and database rules apply. Five follow-ups over the next 64 days drew no further reply, and the embargo of 28 September 2026 passed.

The correspondence also contains three delivery failures: kommunikation@zdf.de rejected the first two messages, and a wrong EDPS address (edps@europa.eu) rejected the copy of 31 August. This report publishes 19 days after the embargo with the full record intact.

ID	Severity	Title
H1	HIGH	Hardcoded Firebase/Google API key and production Realtime Database URL in the app resources
H2	HIGH	Advertising identifier (AD_ID) declared by a fee-funded app that is advertising-free by statute
M1	MEDIUM	Adjust attribution SDK embedded in a public-service app
M2	MEDIUM	Firebase initialisation before the consent screen, with Firebase Authentication and Firestore integrated

Subject & Operator Context

ZDF (Zweites Deutsches Fernsehen), Mainz, is a public-service broadcaster financed by the Rundfunkbeitrag under § 10 RBStV. Its telemedia offering is operated without advertising and sponsoring under the Medienstaatsvertrag. The disclosure went to ZDF's data protection mailbox datenschutz@zdf.de. The original letter named LfDI Rheinland-Pfalz as supervisory authority. ZDF's reply states that LfDI Rheinland-Pfalz has no jurisdiction over ZDF and does not name the competent body. RFI-IRFOS records that correction and does not contest it.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to datenschutz@zdf.de and kommunikation@zdf.de, with presse@zdf.de, the Austrian Datenschutzbehörde, CERT.at, the EDPS and LfDI Rheinland-Pfalz in CC, stating an embargo date of 28 September 2026 and a reply deadline of 14 July 2026. The letter presented one Critical and three High findings and asked three questions: on which Art. 6(1) basis and for which public-service purpose the advertising identifier is processed; whether broadcasting-contribution funds are spent on paid install campaigns measured through Adjust, and if not for which purpose the SDK is used; and which Art. 44-49 transfer mechanism covers Firebase and whether the supervisory authority was informed under Art. 33.

The original letter also contained an engagement-offer section. ZDF's reply noted that it does not use paid services and that security and data protection notes may be reported to ZDF free of charge. RFI-IRFOS's follow-ups did not repeat any commercial offer, and this report contains none.

Re-scoring note: the original letter used the labels C1 (Critical), H1, H2, H3 (High). This report applies CVSS v4.0 consistently. C1 is now H1 (High, impact depends on key restrictions and database rules, a point ZDF's reply also made). The original H1 is now H2 (High, with a stated blast-radius escalation). The original H2 (Adjust) is now M1 and the original H3 (Firebase) is now M2, both Medium, because the presence of a component does not by itself establish processing. Items the original letter reserved for official cooperation remain unpublished.

Eight messages were sent in total (30 June, 6 July, 10 July, 27 July, 31 July, 15 August, 31 August and 12 September 2026).

Findings

H1: Hardcoded Firebase/Google API key and production Realtime Database URL in the app resources

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 - impact depends on key restrictions and database rules, ZDF to state both

```
res/values/strings.xml:
  google_api_key:      [REDACTED IN PUBLIC REPORT -- disclosed privately to ZDF in
                        R1]
  firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to ZDF in
                        R1]
Reachable by: any party decompiling the published APK
```

Impact: A Google/Firebase API key and the production Firebase Realtime Database URL are hardcoded in res/values/strings.xml of the published APK. Both values are withheld from this public report; they were disclosed privately to ZDF in the original R1 letter. An unrestricted key enables quota and billing exhaustion against the underlying Google Cloud project, and the database URL establishes a conditional read path if the Realtime Database security rules are not deny-by-default. ZDF's reply of 10 July 2026 states that the presence of a Firebase API key does not by itself constitute a vulnerability and that the assessment depends on the concrete configuration. RFI-IRFOS agrees with that framing: the exploitable impact depends on two facts only ZDF can state, namely the restrictions applied to the key and the database security rules. The original disclosure labelled this finding CRITICAL; this report scores it HIGH under CVSS v4.0 for that reason.

H2: Advertising identifier (AD_ID) declared by a fee-funded app that is advertising-free by statute

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, 5.3 - permission declared, purpose for the advertising identifier undocumented

```
<uses-permission android:name="com.google.android.gms.permission.AD_ID"/>  
Operator financing: Rundfunkbeitrag (§ 10 RBStV)  
Telemedia offering: advertising- and sponsoring-free (§ 30 MStV)
```

Impact: The manifest declares com.google.android.gms.permission.AD_ID, the Google advertising identifier, a persistent device-linked ID designed for cross-app advertising profiling. ZDF is financed by the broadcasting contribution (Rundfunkbeitrag) and operates its telemedia offering without advertising or sponsoring under the Medienstaatsvertrag. ZDF's reply of 10 July 2026 names Art. 6(1)(e) GDPR, together with ZDF's statutory duties under the Medienstaatsvertrag to offer contemporary telemedia and to carry out performance analyses, as the basis for its usage measurement, and notes that the declaration of a permission does not by itself establish processing. That reply explains usage measurement. It does not explain why the advertising identifier specifically is declared, which purpose it serves, or whether it is read. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.3 to HIGH because the app is financed by a mandatory broadcasting contribution, serves the general public with no ad-free alternative to opt into, and is subject to a statutory advertising ban that makes any advertising-identifier use a purpose-limitation question.

M1: Adjust attribution SDK embedded in a public-service app

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 - SDK presence and early start, purpose undocumented

```
smali/com/adjust/, smali_classes3/com/adjust/sdk/  
com.adjust.sdk.SystemLifecycleContentProvider (ContentProvider, starts with the  
process)  
com.adjust.sdk.AdjustConfig
```

Impact: The Adjust SDK is embedded, with com.adjust.sdk.SystemLifecycleContentProvider declared as a ContentProvider that starts with the process, before any consent screen can be answered. Adjust is a commercial attribution SDK, typically used to measure which paid install campaigns led to which installs. RFI-IRFOS asked whether broadcasting-contribution funds are spent on paid install campaigns measured through Adjust and, if not, for which purpose the SDK is used and where that purpose is documented. ZDF's reply does not address Adjust by name. ZDF also stated that the presence of an SDK does not by itself establish processing, which is correct as a matter of logic and is the reason this finding carries MEDIUM severity.

M2: Firebase initialisation before the consent screen, with Firebase Authentication and Firestore integrated

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 - early start and US infrastructure, transfer mechanism undocumented

```
<provider android:name="com.google.firebase.provider.FirebaseInitProvider"
    android:initOrder="100" android:directBootAware="true"/>
Firebase Authentication: 5 smali classes    Firestore: 4 smali classes
```

Impact: com.google.firebase.provider.FirebaseInitProvider (initOrder 100, directBootAware) starts before the app logic and before the consent screen. Firebase Authentication (5 smali classes) and Firebase Firestore (4 smali classes) are integrated, so user authentication and potentially user data run through Google infrastructure in the United States. RFI-IRFOS asked which Art. 44-49 transfer mechanism covers this and whether the competent supervisory authority has been informed. ZDF's reply states that conclusions about third-country transfers cannot be drawn from the presence of an SDK, and does not name a transfer mechanism.

Impact Analysis

The findings are fixable engineering and documentation gaps, and the ZDF reply is right that a permission, an SDK or a key does not by itself prove misuse. What the report asks for are the facts only ZDF holds: the key restrictions and database rules, the purpose of the advertising identifier, the Adjust budget question and the Firebase transfer mechanism. The correspondence shows one substantive position taken early, and silence on those facts afterwards.

The Complete Chain: Eight Messages, 74 Days, One Reply, Five Follow-ups Unanswered

Step 1 – Disclosure sent: RFI-IRFOS sends the full findings on 30 June 2026 to datenschutz@zdf.de and kommunikation@zdf.de, with presse@zdf.de, the Austrian Datenschutzbehoerde, CERT.at, the EDPS and LfDI Rheinland-Pfalz in CC. kommunikation@zdf.de rejects the message.

Step 2 – First follow-up: on 6 July 2026 RFI-IRFOS repeats the findings. kommunikation@zdf.de rejects it again.

Step 3 – The reply: on 10 July 2026 ZDF's data protection officer replies. The reply disputes the assessments, names the basis for usage measurement, states that a key, permission or SDK alone does not establish a vulnerability or processing, states that LfDI Rheinland-Pfalz has no jurisdiction, declines paid services and declines to give information on internal architecture, security measures and contracts. RFI-IRFOS responds the same day.

Step 4 – Silence after the reply: follow-ups on 27 July, 31 July, 15 August, 31 August and 12 September 2026 restate the open points. No reply to any of them.

Step 5 – Address correction: the copy of 31 August to edps@europa.eu is rejected because the address is wrong. The correct address is edps@edps.europa.eu.

Step 6 – Embargo passes: 28 September 2026 passes with the open points unanswered.

Step 7 – Publication: this report publishes 19 days after the embargo, with eight messages sent, one reply received and the specific questions on the advertising identifier, Adjust, Firebase transfers and key restrictions still open.

Data Protection – Article by Article

Art. 32(1)(b) GDPR – Security of processing: H1's hardcoded key and database URL; the exploitable impact depends on the key restrictions and database rules.

Art. 5(1)(b), Art. 6(1) and Art. 13 GDPR – Purpose limitation, lawfulness and transparency: H2's advertising identifier on an advertising-free, fee-funded app. ZDF names Art. 6(1)(e) for usage measurement; the purpose of the advertising identifier itself is not explained.

Art. 7 and Art. 13 GDPR – Consent and transparency: M1's Adjust provider and M2's Firebase provider start before the consent screen.

Art. 44-49 GDPR – Third-country transfers: M2's Firebase Authentication and Firestore run through Google infrastructure in the United States; no transfer mechanism was named.

Art. 33 GDPR – ZDF's reply states that no notifiable personal data breach arises from the message. RFI-IRFOS did not allege a breach; the Art. 33 reference in the original letter was a question about notification practice.

Regulatory & Legal Landscape

ZDF stated on 10 July 2026 that LfDI Rheinland-Pfalz has no jurisdiction over ZDF and did not name the competent supervisory body. RFI-IRFOS records the correction. The Austrian Datenschutzbehörde, CERT.at, the EDPS and LfDI Rheinland-Pfalz were in CC on the original disclosure and on the follow-ups through 31 August 2026. The follow-up of 12 September 2026 went to ZDF with presse@zdf.de in copy.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32 issue in H1, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 5, 6, 7, 13 and 44-49 questions in H2, M1 and M2, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Whether and how these provisions apply to ZDF depends on the competent supervisory arrangements that ZDF's reply did not describe.

Indicators of Compromise

The following items were extracted from the published production APK via static analysis only. No ZDF servers, accounts, or infrastructure were probed. The Firebase/Google API key and the Realtime Database URL referenced in H1 are withheld from this public report; full values were disclosed privately to ZDF in the original R1 letter.

```
H1 -- res/values/strings.xml: google_api_key and firebase_database_url (redacted)
H2 -- AndroidManifest.xml: com.google.android.gms.permission.AD_ID
M1 -- com.adjust.sdk.SystemLifecycleContentProvider, com.adjust.sdk.AdjustConfig
M2 -- com.google.firebase.provider.FirebaseInitProvider (initOrder=100),
     Firebase Authentication (5 classes), Firestore (4 classes)
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to datenschutz@zdf.de and kommunikation@zdf.de, CC presse@zdf.de, Austrian Datenschutzbehörde, CERT.at, EDPS and LfDI Rheinland-Pfalz. Embargo stated as 2026-09-28. kommunikation@zdf.de rejects the message (550 5.1.1, address not found).

2026-07-06 Follow-up sent to the same addresses. kommunikation@zdf.de rejects it again.

2026-07-10 ZDF's data protection officer replies for the first and only time (details in the section above). Same day, RFI-IRFOS responds to ZDF and all parties in copy.

2026-07-27 Follow-up sent to datenschutz@zdf.de, CC unchanged. No reply.

2026-07-31 Second-round follow-up (R2) sent. No reply.

2026-08-15 Follow-up sent, noting the self-set reply deadline of 2026-08-05 had passed. No reply.

2026-08-31 Follow-up sent. The copy to edps@europa.eu is rejected (550 5.1.1), a wrong address; the correct EDPS address is edps@edps.europa.eu. No reply.

2026-09-12 Follow-up sent, 74 days since the original disclosure, CC presse@zdf.de. No reply.

2026-09-28 Embargo date reached and passed. No further reply after 2026-07-10.

2026-10-17 This report published, 19 days after the embargo date. Correspondence record: eight RFI-IRFOS messages, one reply (2026-07-10), three delivery failures, no reply to any follow-up.

Residual Risk & Recommendations

H1 – Confirm that the Firebase/Google API key is restricted to the production signing certificate and the APIs actually used, confirm that the Realtime Database rules are deny-by-default and locked to authenticated access, and rotate the key.

H2 – Document the purpose of the declared advertising identifier, or remove the AD_ID permission if no advertising or attribution use exists.

M1 – State whether Adjust is used for paid install attribution and where its purpose is documented in the privacy information, or remove the SDK.

M2 – Defer Firebase initialisation until the consent decision is recorded, and name the Art. 44-49 transfer mechanism for Firebase Authentication and Firestore in the privacy information.

Procedural: the key restriction and database rule facts in H1 are the quickest way to close the most serious open point. RFI-IRFOS remains open to a substantive reply to the specific questions 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 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of the published application using publicly available tooling. No ZDF servers, accounts, or infrastructure were probed. The credential values referenced in H1 are withheld from this public report and were disclosed privately to ZDF in the original R1 letter. ZDF's positions in this report are summarised from its reply of 10 July 2026. Analysis by RFI-IRFOS, ZVR 1015608684, GISA 39261441, Steuernummer 68 696/8736. REF COM.ZDF.ANDROID.MEDIATHEK.