Coordinated Security & Privacy Disclosure, Final Report

BILD News App for Android (com.netbiscuits.bild.android, v9.21)

Eight written notices, a bug-bounty redirect, a personal-data objection, a two-way regulator jurisdiction dispute, ninety-five days, zero substantive technical answers

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FOUR FINDINGS UNADDRESSED AFTER EIGHT NOTICES AND THREE PERSONAL REPLIES

Target	Axel Springer SE / Axel Springer Deutschland GmbH
Product audited	BILD News App for Android, com.netbiscuits.bild.android, v9.21 (versionCode 1514224)
Disclosure reference	REF BILD-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C1 a hardcoded, never-rotated Firebase key capable of forging push notifications to 40 million-plus readers, CVSS v4.0 8.8, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production BILD News App Android application and identified one CRITICAL and three HIGH findings: a Firebase API key hardcoded in the shipped APK, tied to an auto-generated Google Cloud project name never renamed since first integration, indicating the key was never rotated, capable of forging push notifications to BILD's 40 million-plus reader base and reading Remote Config paywall and feature-flag data, a Network Security Configuration domain exception permitting cleartext traffic for a private developer test IP address (192.168.1.41) apparently committed into the production binary by mistake, with no certificate pinning on any BILD endpoint, an active Google Topics API on a political news platform with no Art. 9 consent architecture, meaning ad-topic categories inferred from a user's reading behavior on political news constitute special-category data with no matching consent gate, and a seven-vendor advertising-technology stack (3,354 combined smali classes) of which five vendors are US-based, with no documented Art. 46 transfer mechanism cited for the resulting international data transfers.

Axel Springer's internal privacy team replied personally twice within three days of R1, first redirecting RFI-IRFOS to the company's Intigriti bug-bounty portal, a channel RFI-IRFOS declined as inapplicable to a formal GDPR notice, then promising an internal review 'as soon as possible' and naming the company's Data Protection Officer as an escalation contact. Twenty-three days later, that named DPO contact replied once, but solely to object to being personally identified in connection with these findings on RFI-IRFOS's public disclosure ledger, citing a right to erasure of that personal reference, without commenting on any of the four technical findings themselves. RFI-IRFOS additionally pursued a jurisdictional path through the BfDI, which twice declined jurisdiction and redirected to Berlin's data protection authority, whose only reply was generic complaint-filing guidance rather than confirmation of an opened case file. Across eight written notices and ninety-five days, none of the four technical findings ever received a substantive answer.

Scope: Static analysis of the publicly downloaded production BILD News App Android APK (v9.21), on an authorized test device, only. No Axel Springer account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@axelspringer.de, bcc the Austrian Datenschutzbehoerde, CERT.at, and Berlin's data protection authority. Axel Springer's internal privacy team replied personally twice, first redirecting to a bug-bounty portal, then promising an internal review 'as soon as possible.' Twenty-three days later, the named DPO contact replied once, but solely to object to being personally identified on RFI-IRFOS's public disclosure ledger, without commenting on any of the four technical findings. No substantive technical answer was ever received across eight written notices and ninety-five days, and a jurisdictional dispute between the BfDI and Berlin's data protection authority left the case without a confirmed open regulatory file.

ID	Severity	Title
C1	CRITICAL	Hardcoded, never-rotated Firebase API key in the production APK
H1	HIGH	Developer test IP cleartext exception in the production Network Security Config, no certificate pinning
H2	HIGH	Google Topics API active on a political news platform without Art. 9 consent architecture
H3	HIGH	Seven-vendor advertising-technology stack, five US-based, no documented Art. 46 transfer mechanism

Subject & Operator Analysis

Axel Springer SE, headquartered in Berlin, operates the BILD News App through its subsidiary Axel Springer Deutschland GmbH. Berlin's data protection authority is Axel Springer's lead supervisory authority under GDPR one-stop-shop rules.

Findings

C1: Hardcoded, never-rotated Firebase API key in the production APK

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N, 8.8

google_api_key AIzaSyAuyiK2rcvUprhKkQXKwtzRE6lJqFC3Ybl is hardcoded in res/values/strings.xml, tied to Firebase project 'iconic-mariner-818,' an auto-generated GCP project name never renamed since first integration, indicating the key has never been rotated.

This key can be used to forge push notifications to BILD's 40 million-plus reader base, read Remote Config including paywall thresholds, A/B test parameters, and feature flags, and potentially access session or subscriber data depending on Firebase security rules. No reply of any kind addressed this finding across eight notices.

Impact: A media property with tens of millions of readers carries a phishing and disinformation vector via forged push notifications, in addition to the standard risks a hardcoded Firebase key carries.

Fix: Rotate the exposed key, restrict it to the correct package name and SHA-256 signing fingerprint, and confirm deny-by-default Firebase security rules.

H1: Developer test IP cleartext exception in the production Network Security Config, no certificate pinning

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

The production Network Security Config contains a domain-config entry with cleartextTrafficPermitted="true" for 192.168.1.41, a typical consumer-router DHCP address, apparently a developer local-test exception committed into the production binary by mistake. No SHA-256 certificate pinning exists on any BILD endpoint.

No reply of any kind addressed this finding.

Impact: A development artifact left in a production release configuration, combined with the complete absence of certificate pinning, leaves all BILD traffic susceptible to interception on any untrusted network.

Fix: Remove the developer test IP exception from the production Network Security Config and implement certificate pinning.

H2: Google Topics API active on a political news platform without Art. 9 consent architecture

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

The app requests ACCESS_ADSERVICES_TOPICS. On a political news app, resulting topic categories reflect political reading behavior, special-category data under Art. 9. The ga_ad_services_config.xml is empty, so none of the app's seven ad-tech SDKs are restricted from querying Topics data.

No reply of any kind addressed this finding.

Impact: Political-opinion-adjacent special-category data may be inferable via the Topics API by any of seven bundled ad-tech vendors with no restriction and no confirmed Art. 9(2)(a) consent gate.

Fix: Populate ga_ad_services_config.xml to restrict Topics API access, and deploy an explicit Art. 9(2)(a) consent gate before any political-content-derived topic categories are shared.

H3: Seven-vendor advertising-technology stack, five US-based, no documented Art. 46 transfer mechanism

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

3,354 combined smali classes implement Teads (Luxembourg), Sourcepoint (New York, also the app's consent-management tool), Braze (New York), Permutive (London), AppsFlyer (Tel Aviv), AppNexus/Xandr (New York), and Mixpanel (San Francisco). Five of the seven vendors are US-based.

No documented Art. 46 standard-contractual-clause basis was found for the resulting US transfers. No reply of any kind addressed this finding.

Impact: Reader data from a major political news platform may be transferred to five US-based advertising vendors with no documented transfer mechanism.

Fix: Document and publish the Art. 46 transfer mechanism covering each US-based vendor, or restrict data sharing pending that documentation.

Two Personal Replies, One Personal-Data Objection, Zero Technical Answers

Axel Springer's internal privacy team engaged personally and promptly at first, replying within a day of R1 to redirect toward a bug-bounty portal, then again two days later promising an internal review and naming a DPO contact. Three weeks after that promise, the named DPO contact replied once, but the reply addressed only a personal-data concern, an objection to being individually identified in connection with these findings on RFI-IRFOS's public disclosure ledger, and did not comment on any of the four technical findings. RFI-IRFOS separately pursued the BfDI, which twice declined jurisdiction in favor of Berlin's data protection authority; Berlin's only reply was generic complaint-filing guidance rather than confirmation that a case file had been opened. Across eight written notices and ninety-five days, none of the four technical findings ever received a substantive answer from anyone at Axel Springer.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Never-rotated Firebase key capable of forging push to 40M+ readers
H1	GDPR Art. 25, Art. 32(1)	Developer test exception in production NSC, no certificate pinning
H2	GDPR Art. 9(1)/(2)(a); TKG 2021 Sec. 25	Topics API active on political content with no consent architecture
H3	GDPR Art. 13(1)(e), Art. 46	Undocumented US transfer mechanism for five ad-tech vendors

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@axelspringer.de, bcc Austrian DSB/CERT.at/Berlin DPA; 1 CRITICAL + 3 HIGH findings
2026-06-22	Axel Springer's privacy team redirects to the Intigriti bug-bounty portal; RFI-IRFOS declines as inapplicable
2026-06-24	Axel Springer promises an internal review, names the DPO contact
2026-07-17	The DPO contact replies, objecting only to being personally named on the public ledger; no comment on the technical findings
2026-07-20	RFI-IRFOS escalates to the BfDI, which had declined jurisdiction; Berlin DPA replies with generic complaint-filing guidance
2026-08-19	Formal complaint filed with Berlin DPA; BfDI again declines jurisdiction under a second case reference
2026-09-04	Follow-up, seventy-three days since the review promise, last message on file
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Provide a substantive technical answer to each of the four findings, separate from the personal-data objection already addressed.
- Rotate the exposed Firebase key and restrict it to the correct package name and signing fingerprint.
- Remove the developer test IP exception from the production Network Security Config and implement certificate pinning.
- Populate ga_ad_services_config.xml and deploy an explicit Art. 9(2)(a) consent gate for Topics API data on political content.
- Document the Art. 46 transfer mechanism for each US-based ad-tech vendor.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. GDPR Art. 9, 13, 25, 32, 46. TKG 2021 Sec. 25. REF BILD-2026-R1.