Coordinated Security & Privacy Disclosure, Final Report

DER SPIEGEL for Android (de.spiegel.android.app.spon, v5.3.1, versionCode 224)

Six written notices, a regulator that never received the disclosure through the company's own queue, ninety days, zero substantive replies from the operator

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FOUR FINDINGS UNADDRESSED, DISCLOSURE NEVER REACHED THE LEAD REGULATOR THROUGH THE OPERATOR'S OWN QUEUE

Target	SPIEGEL-Verlag Rudolf Augstein GmbH & Co. KG / Spiegel-Gruppe, Hamburg, Germany
Product audited	DER SPIEGEL for Android, de.spiegel.android.app.spon, v5.3.1 (versionCode 224)
Disclosure reference	REF SPIEGEL-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (H1 cleartext traffic permitted for main production domains with no certificate pinning, CVSS v4.0 8.6, 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 DER SPIEGEL Android application and identified one CRITICAL, two HIGH, and one MEDIUM finding: a Firebase API key hardcoded in the shipped APK tied to a deliberately-named project, spiegel-online-tracking, confirming the backend's purpose rather than an auto-generated placeholder, a Network Security Configuration permitting cleartext HTTP traffic for the main production domains spiegel.de and manager-magazin.de, plus a Triton Digital/iHeartMedia US advertising endpoint, with no certificate pinning on any endpoint, an active Google Topics API on a political-investigative news outlet with no ad_services_config.xml restriction and no identified Art. 9(2)(a) consent flow, meaning interest categories inferred from political reporting readership constitute special-category data, and a privacy policy that does not disclose Topics-API-derived interest profiling or its legal basis.

Across six written notices over ninety days, Spiegel-Gruppe's Zendesk-ticketed privacy inbox returned only two identical automated subscription-management auto-replies, and the operator itself never sent a substantive human reply. On 3 August, Hamburg's data protection authority contacted RFI-IRFOS directly to clarify that, despite RFI-IRFOS's own correspondence stating the disclosure had already been filed with them as the competent supervisory authority, no such disclosure had actually reached them, RFI-IRFOS's bcc attempt to the correct Hamburg DPA address had failed silently while an earlier attempt to a nonexistent domain had bounced audibly. RFI-IRFOS corrected the routing the same day and restated all findings directly to Hamburg's DPA. None of RFI-IRFOS's three standing questions, on the Art. 6/7 legal basis for political-interest profiling via Topics API, DPO awareness independent of the Zendesk auto-replies, or a documented Art. 35 DPIA, ever received an answer from the operator.

Scope: Static analysis of the publicly downloaded production DER SPIEGEL Android APK (v5.3.1), on an authorized test device, only. No SPIEGEL account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@spiegelgruppe.de, a Zendesk-ticketed inbox, bcc the Austrian Datenschutzbehoerde, CERT.at, and Hamburg's data protection authority (bounced, incorrect address). Across six written notices over ninety days, Spiegel-Gruppe's Zendesk queue returned only two identical automated subscription-management auto-replies. On 3 August, Hamburg's data protection authority contacted RFI-IRFOS directly, stating that despite being told a disclosure had been filed with them as the competent authority, no such disclosure had actually arrived, RFI-IRFOS's bcc attempt to the correct Hamburg DPA address had itself failed silently.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded, project deliberately named 'spiegel-online-tracking'
H1	HIGH	Network Security Config permits cleartext HTTP for main production domains, no certificate pinning

ID	Severity	Title
H2	HIGH	Google Topics API active on a political-investigative news outlet without safeguards
M1	MEDIUM	Privacy policy does not disclose Topics API processing

Subject & Operator Analysis

SPIEGEL-Verlag Rudolf Augstein GmbH & Co. KG, part of the Spiegel-Gruppe, is headquartered in Hamburg, Germany. Hamburg's data protection authority (HmbBfDI) is the operator's lead supervisory authority under GDPR one-stop-shop rules.

Findings

C1: Firebase API key hardcoded, project deliberately named 'spiegel-online-tracking'

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N, 6.9

google_api_key AIzaSyDcCQH5r1W0C9uc8b6wywOHMJ1qtekLif4 and firebase_database_url https://spiegel-online-tracking.firebaseio.com are hardcoded in res/values/strings.xml. The project name was deliberately chosen by developers, not auto-generated, confirming the backend's tracking purpose.

No reply of any kind, from the operator, addressed this finding across six notices.

Impact: A deliberately-named tracking project's attack surface cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Rotate the exposed key, confirm deny-by-default security rules, and enforce App Check for this project.

H1: Network Security Config permits cleartext HTTP for main production domains, 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

Domain-config entries declare `cleartextTrafficPermitted="true"` for spiegel.de, manager-magazin.de, and mc.tritondigital.com (Triton Digital/iHeartMedia, US). No base-config and no SHA-256 certificate pin exist for any endpoint.

No reply of any kind addressed this finding.

Impact: Traffic to the publication's own primary domains, and to a third-party US advertising vendor, can be transmitted in cleartext and intercepted or altered on any untrusted network.

Fix: Remove the cleartext exceptions for production domains and implement certificate pinning.

H2: Google Topics API active on a political-investigative news outlet without safeguards

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 uses the Google Topics API to build interest categories from app usage. On a political-investigative outlet, resulting categories directly reflect political opinions, special-category data under GDPR Art. 9. No ad_services_config.xml restricting SDK access to Topics data, and no explicit Art. 9(2)(a) consent flow, was identified.

No reply of any kind addressed this finding.

Impact: Political-opinion-adjacent special-category data may be inferable via the Topics API with no confirmed Art. 9(2)(a) consent gate on a platform whose core content is political and investigative journalism.

Fix: Restrict Topics API access via ad_services_config.xml and deploy an explicit Art. 9(2)(a) consent gate.

M1: Privacy policy does not disclose Topics API processing

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, 6.9

The privacy policy names no legal basis or disclosure for Topics-API-derived political interest profiling, an Art. 13 GDPR concern raised in the 3 August follow-up.

No reply of any kind addressed this finding.

Impact: Users have no way to learn, from the privacy policy itself, that political-reading-derived interest categories are being generated at all.

Fix: Add explicit disclosure of Topics API processing and its legal basis to the privacy policy.

The Disclosure That Never Reached Its Own Regulator

On 3 August, Hamburg's data protection authority (HmbBfDI, represented by Marius Zirngibl) contacted RFI-IRFOS directly: it had been told a disclosure concerning security problems in the SPIEGEL Android app had already been filed with it as the competent authority, but no such disclosure had actually arrived. RFI-IRFOS's own correspondence traced the gap: the 21 June, 28 June, and 24 July sends had all gone to Spiegel-Gruppe's Zendesk-ticketed privacy queue, and a bcc attempt to Hamburg's data protection authority had used an incorrect domain that bounced, silently, with the failure notification easy to miss among other automated traffic. RFI-IRFOS corrected the routing the same day and restated all findings directly to the DPA. Spiegel-Gruppe itself, across six notices and ninety days, never sent a substantive human reply of its own, only two identical automated Zendesk subscription-management auto-replies.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Hardcoded key for a deliberately-named tracking project
H1	GDPR Art. 32(1)(a)	Cleartext traffic permitted for main production domains, no certificate pinning
H2	GDPR Art. 9(1)/(2)(a)	Topics API political-interest profiling with no consent gate
M1	GDPR Art. 13	Privacy policy silent on Topics API processing

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@spiegelgruppe.de (Zendesk queue), bcc Austrian DSB/CERT.at/Hamburg DPA (bounced, wrong domain); automated Zendesk auto-reply
2026-06-28	Follow-up sent, bcc attempt to Hamburg DPA bounces again; second automated auto-reply
2026-08-03	Hamburg's DPA contacts RFI-IRFOS directly, confirms no disclosure had reached it; RFI-IRFOS corrects routing the same day and restates all findings
2026-08-15	Follow-up, fifty-five days, twenty-three days since the routing correction, cc Hamburg DPA correctly
2026-09-06	Follow-up, seventy-seven days, notes the only reply this case ever produced from the operator was a subscription-management bot
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Route GDPR disclosures received through the Zendesk queue to a human privacy contact, distinct from subscriber-support ticketing.
- Remove cleartext exceptions for spiegel.de, manager-magazin.de, and the Triton Digital endpoint, and implement certificate pinning.
- Restrict Topics API access via ad_services_config.xml and deploy an explicit Art. 9(2)(a) consent gate.
- Add explicit privacy-policy disclosure of Topics API processing.
- Rotate the exposed Firebase key.

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, 32. REF SPIEGEL-2026-R1.