Coordinated Security & Privacy Disclosure, Final Report

mein dm for Android (de.dm.meindm.android)

Seven written notices, ninety days, one automated receipt confirmation from the lead regulator only, zero replies from dm itself

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SIX FINDINGS UNADDRESSED AFTER SEVEN NOTICES

Target	dm-drogerie markt GmbH & Co. KG, Karlsruhe, Germany, and dm Austria GmbH
Product audited	mein dm for Android, de.dm.meindm.android
Disclosure reference	REF MEINDM-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 three US advertising SDKs integrated on Art. 9-inferable drugstore purchase data, CVSS v4.0 8.7, 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 mein dm Android application and identified two CRITICAL and three HIGH findings, plus one MEDIUM finding: a Firebase project key hardcoded in the shipped APK, three US advertising SDKs (AppLovin, IronSource, Chartboost) integrated on purchase data capable of Art. 9 inference (baby/prenatal products, over-the-counter medication, contraceptives, kosher/halal/organic groceries, and Naturheilkunde/homeopathic remedies), an Adjust purchase-verification integration whose own internal strings confirm persistent storage of purchase events linked via the Google Advertising ID even after a user has exercised their right to erasure, advertising-ID permissions enabling cross-app linkage of that same health-inferable purchase data, Firebase Analytics/Crashlytics/Messaging sending behavioral and device data to Google in the US with no identified Art. 13(1)(e) disclosure, and an absence of certificate pinning on loyalty-credential and receipt-data endpoints.

Across seven written notices over ninety days, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde, CERT.at, and LfDI Baden-Wuerttemberg as dm's designated lead supervisory authority, the only inbound message in this case was a single automated receipt confirmation from LfDI Baden-Wuerttemberg itself, received the same day R1 was sent. dm-drogerie markt never responded at any point, not even with an automated acknowledgment. None of RFI-IRFOS's five standing questions, on Firebase key rotation, an Art. 35 DPIA covering the three advertising networks, the Art. 9(2) legal basis for transferring drugstore purchase data to them, whether dm would act before or after LfDI contact, or Art. 33 notification within 72 hours, ever received a reply.

Scope: Static analysis of the publicly downloaded production mein dm Android APK, on an authorized test device, only. No dm account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@dm.de, bcc dsb@dsb.gv.at, cert@cert.at, and poststelle@lfdi.bwl.de (LfDI Baden-Wuerttemberg, dm's designated lead supervisory authority). Across seven written notices over ninety days, the only inbound message of any kind was a single automated receipt confirmation from LfDI Baden-Wuerttemberg itself, received the same day R1 was sent. dm-drogerie markt never responded, not even with an automated acknowledgment.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the production APK
C2	CRITICAL	Three US advertising SDKs integrated on Art. 9-inferable drugstore purchase data
H1	HIGH	Adjust purchase-verification integration retains purchase events after erasure requests
H2	HIGH	Advertising-ID permissions enabling cross-app linkage of health-inferable data

ID	Severity	Title
H3	HIGH	Firebase Analytics, Crashlytics, and Messaging send behavioral data to Google without explicit Art. 13 disclosure
M1	MEDIUM	No certificate pinning on loyalty and receipt-data endpoints

Subject & Operator Analysis

dm-drogerie markt GmbH & Co. KG operates as a German drugstore chain headquartered in Karlsruhe, with dm Austria GmbH as its Austrian subsidiary. LfDI Baden-Wuerttemberg is dm's designated lead supervisory authority under GDPR one-stop-shop rules.

Findings

C1: Firebase API key hardcoded in the production APK

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

res/values/google-services.xml contains hardcoded key AIzaSyDy2h3Pyct4drQgxNr_L8ata4gBri91mIo, Firebase project mein-dm (GCP #27845377631), appId 1:2784537763 1:android:29441c5515d024f4bd65ea, storage bucket mein-dm.firebasestorage.app.

No reply of any kind, from dm or any recipient, addressed this finding across seven notices.

Impact: A production Firebase 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 Firestore/RTDB security rules are deny-by-default, and enforce App Check for this project.

C2: Three US advertising SDKs integrated on Art. 9-inferable drugstore purchase data

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

com.applovin.sdk.*, com.ironsource.mediationsdk.*, and com.chartboost.* are present alongside purchase-data processing capable of revealing pregnancy status, health conditions, or religious affiliation, baby/prenatal products, over-the-counter medication, contraceptives, kosher/halal/organic groceries, and Naturheilkunde remedies. No evidence of an Art. 35 DPIA covering the three networks was found. The Chartboost SDK itself ships GDPR/CCPA consent-model classes, indicating awareness of the regulatory sensitivity of this data.

No reply of any kind addressed this finding.

Impact: Special-category data may be inferable by third-party advertising networks from ordinary drugstore purchases with no documented Art. 9(2) legal basis or DPIA covering that specific processing.

Fix: Conduct and publish an Art. 35 DPIA covering all three advertising networks, or exclude Art. 9-inferable product categories from data shared with them.

H1: Adjust purchase-verification integration retains purchase events after erasure requests

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

Internal strings AdjustPurchaseVerificationResult, 'Added purchase_verification %d', 'Purchase verification aborted because event instance is null', and 'Purchase verification aborted because user is GDPR forgotten' confirm persistent storage of purchase events linked via the Google Advertising ID, and confirm the app's own code is aware of, and checks for, a user's erasure status.

The presence of the 'GDPR forgotten' check demonstrates the retention itself is a known, deliberate design property rather than an oversight. No reply of any kind addressed this finding.

Impact: Purchase-event data linked to Art. 9-inferable categories may persist and remain linkable via GAID even where a user has exercised their Art. 17 right to erasure through other channels.

Fix: Extend erasure handling to purge stored purchase-verification events, not only abort future processing of them.

H2: Advertising-ID permissions enabling cross-app linkage of health-inferable data

---

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

AD_ID, ACCESS_ADSERVICES_AD_ID, and ACCESS_ADSERVICES_ATTRIBUTION permissions are present in combination with the Art. 9-relevant purchase data described in C2.

No reply of any kind addressed this finding.

Impact: Advertising-identifier permissions enable cross-app profile linkage of purchase data that can reveal special-category information.

Fix: Deploy a consent-management platform gating advertising-identifier collection specifically for Art. 9-inferable product categories.

H3: Firebase Analytics, Crashlytics, and Messaging send behavioral data to Google without explicit Art. 13 disclosure

---

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

No explicit Art. 13(1)(e) disclosure was identified for behavioral and device data flowing to Google (US) via bundled Firebase Analytics, Crashlytics, and Messaging.

No reply of any kind addressed this finding.

Impact: Behavioral and device data may be transferred to a named third party without a matching disclosure of that specific recipient.

Fix: Name Google Firebase Analytics, Crashlytics, and Messaging explicitly as recipients in the app's privacy notice.

M1: No certificate pinning on loyalty and receipt-data endpoints

---

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3

The Network Security Config relies on system CAs only; loyalty credentials and receipt-data endpoints are unprotected against interception via an MDM-installed or otherwise rogue certificate authority.

No reply of any kind addressed this finding.

Impact: Loyalty and receipt data traffic can be intercepted on a device where a rogue certificate authority is trusted.

Fix: Implement certificate pinning for loyalty-credential and receipt-data endpoints.

Seven Notices, One Regulator Receipt, Zero Replies From dm

The only inbound message this case produced across seven notices and ninety days was a single automated receipt confirmation from LfDI Baden-Wuerttemberg, dm's own lead supervisory authority, received the same day R1 was sent. dm-drogerie markt itself never responded at any point in the sequence, not even with an automated acknowledgment of its own. Seven notices over ninety days produced silence from the company named in the disclosure.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded Firebase key in the production APK
C2	GDPR Art. 9, Art. 35	Undocumented DPIA for Art. 9-inferable purchase data shared with three ad networks
H1	GDPR Art. 17	Purchase-event retention surviving an erasure request
H2	GDPR Art. 9, Art. 13(1)(e)(f)	Cross-app linkage of health-inferable purchase data
H3	GDPR Art. 13(1)(e)	Undisclosed behavioral data transfer to Google
M1	GDPR Art. 32	No certificate pinning on loyalty/receipt endpoints

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@dm.de, bcc Austrian DSB/CERT.at/LfDI Baden-Wuerttemberg; 2 CRITICAL + 3 HIGH + 1 MEDIUM findings; automated receipt confirmation from LfDI same day
2026-06-28	Follow-up #1, seven days, no reply, three questions posed
2026-07-17	Follow-up #2, twenty-six days, notes LfDI confirmed receipt but dm itself never answered
2026-08-24	Follow-up #5, sixty-four days, no single reply, invokes the Art. 33(4) 72-hour breach-notification clock
2026-08-31	Follow-up #6, REF MEINDM-2026-R1, seventy-one days, two regulator notifications, no reply, weekly SHA-256 re-hashing during embargo disclosed
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Name a functional escalation path so a written GDPR disclosure to datenschutz@dm.de reaches a human.
- Conduct and publish an Art. 35 DPIA covering AppLovin, IronSource, and Chartboost for Art. 9-inferable purchase categories.
- Extend erasure handling to purge, not merely abort future processing of, stored purchas e-verification events.
- Rotate the exposed Firebase key and confirm deny-by-default security rules with App Check enforced.
- Implement certificate pinning for loyalty-credential and receipt-data endpoints.

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, 17, 25, 32, 35. REF MEINDM-2026-R1.