Coordinated Security & Privacy Disclosure, Final Report

Pollen-Radar for Android (de.ratiopharm.pollenradar)

Nine written notices, ninety days, one acknowledgment with no technical content, zero of three yes/no questions answered

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FOUR FINDINGS UNADDRESSED, THREE STANDING QUESTIONS NEVER ANSWERED

Target	ratiopharm GmbH, a Teva subsidiary, Ulm, Germany
Product audited	Pollen-Radar for Android, de.ratiopharm.pollenradar
Disclosure reference	REF POLLENRADAR-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 four AWS API Gateway keys hardcoded in the public APK, enabling unlimited billed requests against ratiopharm/Teva's AWS account, 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 Pollen-Radar Android application and identified one CRITICAL and three HIGH findings: four AWS API Gateway keys hardcoded in plaintext across both a production and a dev configuration file, the latter also shipped in the public APK and labeled 'LIVE,' enabling anyone downloading the app to make unlimited API requests billed to ratiopharm/Teva's AWS account and to extract the full pollen database, an allowBackup=true manifest setting with no data-extraction-rules exclusions combined with an unencrypted local SQLite database holding Art. 9-relevant health data (monitored pollen types, location-tied pollen exposure history, saved locations), backed up in full to an undisclosed US-processor cloud service, biometric authentication that gates only the app's UI screen while the underlying unencrypted database file remains readable by anything with filesystem access, including ADB backup extraction, root, or physical device access, and a boot-persistent background service combined with precise location collection that builds a health-linked location profile with no documented Art. 9(2) legal basis beyond a generic privacy-policy purpose statement.

Across nine written notices over ninety days, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde, CERT.at, and LfDI Baden-Wuerttemberg, Teva's Data Privacy team replied once, on 29 July, acknowledging receipt and stating that an internal review had been initiated and that protecting user data was Teva's highest priority, but answering none of RFI-IRFOS's three yes/no technical questions: whether the four AWS keys had been removed and rotated, whether the SQLite database was now encrypted with a key derived from biometric authentication, and whether allowBackup had been set to false or comprehensive data-extraction rules defined. No further substantive reply followed across five subsequent written notices over the following seven weeks; the only other inbound correspondence was automated receipt confirmations from LfDI Baden-Wuerttemberg and out-of-office auto-replies from external counsel.

Scope: Static analysis of the publicly downloaded production Pollen-Radar Android APK, on an authorized test device, only. No ratiopharm/Teva account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to dataprotectionofficer.teva@twobirds.com, cc datenschutz@teva.de, bcc the Austrian Datenschutzbehoerde, CERT.at, and LfDI Baden-Wuerttemberg. Teva's Data Privacy team replied once, on 29 July, acknowledging receipt and stating an internal review had been initiated, but answering none of RFI-IRFOS's three yes/no technical questions. No further substantive reply followed across five subsequent written notices over the following seven weeks.

ID	Severity	Title
C1	CRITICAL	Four AWS API Gateway keys hardcoded in the public APK
H1	HIGH	allowBackup=true plus unencrypted SQLite holding Art. 9 health data

ID	Severity	Title
H2	HIGH	Biometric authentication protects only the UI screen, not the database
H3	HIGH	Boot-persistent background service with precise location builds a health-linked location profile

Subject & Operator Analysis

ratiopharm GmbH, headquartered in Ulm, Germany, is a subsidiary of Teva Pharmaceutical Industries. LfDI Baden-Wuerttemberg is ratiopharm's lead supervisory authority under GDPR one-stop-shop rules.

Findings

C1: Four AWS API Gateway keys hardcoded in the public APK

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

assets/public/assets/config.json (production) and assets/public/assets/config_dev.json (dev, also shipped in the public APK and labeled 'environment': 'LIVE') both contain four plaintext AWS API Gateway keys: forecast2_key, map2_key, metadata_key, and download_key.

Anyone downloading the APK from the Play Store obtains all four keys, enabling unlimited API requests billed to ratiopharm/Teva's AWS account and extraction of the full pollen database. No reply of any kind addressed whether these keys have been removed and rotated.

Impact: An unbounded volume of API requests can be generated against ratiopharm/Teva's own AWS billing account by any party extracting these keys from the public APK.

Fix: Remove all four keys from both configuration files, rotate them, and gate API access through an authenticated backend rather than embedded static keys.

H1: allowBackup=true plus unencrypted SQLite holding Art. 9 health 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

AndroidManifest.xml sets allowBackup="true" with no dataExtractionRules exclusions. The CapacitorSQLite configuration sets androidIsEncryption: false. The resulting local database, monitored pollen types, location-tied pollen exposure history, and saved locations, is stored in plaintext and backed up in full to an undisclosed US-processor cloud service.

No reply of any kind confirmed whether allowBackup has been set to false or comprehensive data-extraction rules defined.

Impact: Health-linked pollen-exposure and location history is both stored unencrypted on-device and backed up in full to an undisclosed cloud processor.

Fix: Set allowBackup to false or define data-extraction rules excluding all health-relevant tables, and encrypt the local database.

H2: Biometric authentication protects only the UI screen, not the database

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1

USE_BIOMETRIC and USE_FINGERPRINT permissions gate app access, but the underlying SQLite file (androidIsEncryption: false) remains readable by anything with filesystem access, ADB backup extraction, root, or physical device access. The biometric key is not used to derive a database encryption key.

No reply of any kind confirmed whether the database is now encrypted with a key derived from biometric authentication.

Impact: The biometric lock creates an appearance of data protection that the underlying storage does not actually provide once filesystem-level access is available.

Fix: Derive a database encryption key from the biometric authentication result, so the database itself, not only the UI, is protected.

H3: Boot-persistent background service with precise location builds a health-linked location profile

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 auto-starts on every device boot via RECEIVE_BOOT_COMPLETED and collects GPS-precision location for pollen forecasts. For a pollen-allergy app, this constitutes health-linked location data capable of revealing sleep, work, and avoidance-pattern locations, with no documented Art. 9(2) legal basis beyond a generic privacy-policy purpose statement.

No reply of any kind addressed this finding.

Impact: A precise, continuously-updated location history tied to an allergy condition may be constructed with no specific Art. 9(2) legal basis for that combination.

Fix: Document a specific Art. 9(2) legal basis for combining precise location with allergy-condition data, or reduce location precision/frequency.

One Acknowledgment, Zero of Three Questions Answered

Teva's Data Privacy team replied once, on 29 July, stating: 'Wir haben Ihren Hinweis auf die von Ihnen beschriebenen, moeglicherweise sicherheitsrelevanten Befunde zur Kenntnis genommen und unverzueglich eine interne Pruefung eingeleitet. Der Schutz personenbezogener Daten unserer Nutzerinnen und Nutzer hat fuer Teva hoechste Prioritaet.' The reply did not answer any of RFI-IRFOS's three yes/no technical questions, on key rotation, database encryption, or the allowBackup setting. No further substantive reply followed across five subsequent notices over the following seven weeks; the only other inbound correspondence was automated receipt confirmations from LfDI Baden-Wuerttemberg and out-of-office auto-replies from external counsel.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Four hardcoded AWS keys enabling unlimited billed requests
H1	GDPR Art. 9(1), Art. 13(1)(e), Art. 32(1), Art. 46	Unencrypted health data backed up to an undisclosed US processor
H2	GDPR Art. 25, Art. 32(1)	Biometric lock that does not protect the underlying database
H3	GDPR Art. 5(1)(b), Art. 9(1); TKG 2021 Sec. 165	Health-linked location profile with no specific legal basis

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to dataprotectionofficer.teva@twobirds.com, cc datenschutz@teva.de, bcc Austrian DSB/CERT.at/LfDI Baden-Wuerttemberg; 1 CRITICAL + 3 HIGH findings
2026-07-29	Teva's Data Privacy team acknowledges receipt, states an internal review is underway; answers none of the three questions
2026-08-09	Follow-up notes the 29 July reply answered none of the three questions
2026-09-12	Follow-up notes an 11 September deadline passed unanswered, sets a new deadline of 16 September, restates weekly APK-hash monitoring and the Art. 33 72-hour framing
2026-09-16	Follow-up stated as likely the last message before publication, all four findings restated unchanged, embargo confirmed three days out
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Answer the three outstanding yes/no technical questions specifically, rather than a general acknowledgment.
- Remove and rotate all four hardcoded AWS API Gateway keys.
- Set allowBackup to false or define comprehensive data-extraction rules excluding health-relevant tables.
- Encrypt the local database with a key derived from biometric authentication.
- Document a specific Art. 9(2) legal basis for combining precise location with allergy-condition data.

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. 5, 9, 13, 25, 32, 46. TKG 2021 Sec. 165. REF POLLENRADAR-2026-R1.