Coordinated Security & Privacy Disclosure, Final Report

Dr. Oetker Rezeptideen for Android (at.oetker.android.rezeptideen, v3.9.3)

Eight written notices, ninety days, total silence – not one reply of any kind

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FOUR FINDINGS UNADDRESSED, ZERO REPLIES OF ANY KIND

Target	Dr. Oetker GmbH
Product audited	Dr. Oetker Rezeptideen for Android, at.oetker.android.rezeptideen, v3.9.3
Disclosure reference	REF DROETKER-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 usesCleartextTraffic enabled with no Network Security Config on an app performing Firebase user authentication, 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 Dr. Oetker Rezeptideen Android application and identified two CRITICAL and two HIGH findings: a Firebase API key hardcoded in the public Play Store binary, android:usesCleartextTraffic="true" declared with no Network Security Configuration present at all, on an app that performs Firebase user authentication, meaning login credentials can potentially be exposed over unencrypted HTTP with no certificate pinning anywhere, an allowBackup=true manifest setting with no backup_rules.xml or data_extraction_rules.xml defined, meaning the app's entire data area, recipes, favorites, cooking history, and Firebase authentication tokens, is backed up in full to Google LLC in the US as an undisclosed third-country transfer, and a Facebook SDK integration (501 smali references) providing social login and behavioral tracking, with recipe-browsing and search-term app events flowing to Meta's advertising graph.

Across eight written notices over ninety days, spanning three different email addresses after datenschutz@oetker.de was confirmed nonexistent via an automated delivery failure, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde, CERT.at, LDI NRW, and the German BfDI, no reply of any kind, human or automated, was ever received from Dr. Oetker GmbH. None of RFI-IRFOS's three standing questions, on whether a Network Security Config has since been implemented, whether the Firebase key has been rotated and restricted, or whether a legal basis and consent gate exists for the Facebook SDK's behavioral analytics, ever received an answer.

Scope: Static analysis of the publicly downloaded production Dr. Oetker Rezeptideen Android APK (v3.9.3), on an authorized test device, only. No Dr. Oetker account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@oetker.de, cc presse@oetker.de, bcc the Austrian Datenschutzbehoerde, CERT.at, LDI NRW, and the German BfDI. Across eight written notices over ninety days, spanning three different email addresses after datenschutz@oetker.de was confirmed nonexistent, no reply of any kind, human or automated, was ever received from Dr. Oetker GmbH.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the public APK
C2	CRITICAL	usesCleartextTraffic enabled with no Network Security Config on an app performing user authentication
H1	HIGH	allowBackup=true with no exclusion rules
H2	HIGH	Facebook SDK (501 smali references): social login and behavioral tracking

Subject & Operator Analysis

Dr. Oetker GmbH is a German food manufacturer whose Rezeptideen (recipe ideas) app is distributed in the Austrian and German markets.

Findings

C1: Firebase API key hardcoded in the public 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

google_api_key AIzaSyDDwpwHKoGPoRMPRoeFokn8yQOCI_44iuI, Firebase project droetker-rezeptideen-phone-at, App ID 1:113022279102:android:08140f0aacbaa760, storage bucket droetker-rezeptideen-phone-at.firebasestorage.app, all present in the public Play Store binary.

No reply of any kind, across eight notices, addressed whether this key has been rotated and restricted.

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, restrict it to the correct package name and SHA-256 signing fingerprint, and confirm deny-by-default security rules.

C2: usesCleartextTraffic enabled with no Network Security Config on an app performing user authentication

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

android:usesCleartextTraffic="true" is declared, and no Network Security Configuration exists at all. Firebase Authentication (user login) is present in the app, and no certificate pinning exists on any endpoint.

No reply of any kind confirmed whether a Network Security Config has since been implemented.

Impact: Login credentials on an app that performs user authentication can potentially be transmitted over unencrypted HTTP and intercepted on any untrusted network.

Fix: Set usesCleartextTraffic to false, add a Network Security Configuration, and implement certificate pinning.

H1: allowBackup=true with no exclusion rules

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

android:allowBackup="true" is declared with no backup_rules.xml or data_extraction_rules.xml defined. The app's entire data area, recipes, favorites, cooking history, and Firebase authentication tokens, is backed up in full to Google LLC in the US.

This is an undisclosed third-country transfer with no matching Art. 13(1)(e)/Art. 46 disclosure. No reply of any kind addressed this finding.

Impact: A user's entire app data, including authentication tokens, is transferred to Google's US infrastructure via cloud backup with no comprehensive exclusion policy or disclosed transfer mechanism.

Fix: Define backup_rules.xml and data_extraction_rules.xml excluding authentication tokens and personal data from cloud backup.

H2: Facebook SDK (501 smali references): social login and behavioral tracking

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.facebook.FacebookButtonBase and com.facebook.GraphRequest are present. App events, recipe browsing and search terms, flow to Meta's advertising graph.

No reply of any kind confirmed whether a legal basis and consent gate exists for this behavioral analytics.

Impact: Recipe-browsing and search behavior may be transmitted to Meta's advertising graph with no confirmed consent gate.

Fix: Deploy a consent-management gate for Facebook SDK behavioral tracking and document the Art. 6(1) legal basis.

Eight Notices, Three Addresses, Total Silence

The original address, datenschutz@oetker.de, was confirmed nonexistent via an automated delivery-failure notification on 17 July, over three weeks after R1 was first sent there. Correspondence then moved to dsgvo-service@oetker.com and, from 18 August, to a third address, oetker-nm@corporate-data-protection.com. Across all three addresses and eight written notices over ninety days, no reply of any kind, human or automated, was ever received from Dr. Oetker GmbH.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Hardcoded Firebase key in the public APK
C2	GDPR Art. 32(1)(a), Art. 25	Cleartext traffic enabled on an app performing user authentication
H1	GDPR Art. 32(1), Art. 13(1)(e), Art. 46	Undisclosed full-data backup to a US processor
H2	GDPR Art. 13(1)(e), Art. 46, Art. 6(1)	Undisclosed behavioral tracking via Facebook SDK

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@oetker.de , cc presse@oetker.de, bcc Austrian DSB/CERT.at/LDI NRW/BfDI; 2 CRITICAL + 2 HIGH findings
2026-07-17	Automated bounce confirms datenschutz@oetker.de does not exist, 26 days after the original notice
2026-07-27	Follow-up to the corrected address dsgvo-service@oetker.com, three questions formally recorded for the first time
2026-08-18	Follow-up, 58 days, six messages, adds a third address (oetker-nm@corporate-data-protection.com), deadline set 25 August
2026-09-05	Follow-up, 76 days since the original notice, deadline set 15 September, embargo reconfirmed unchanged
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Establish a functioning privacy contact, given the publicly listed address does not exist.
- Set usesCleartextTraffic to false, add a Network Security Configuration, and implement certificate pinning.
- Rotate the exposed Firebase key and restrict it to the correct package name and signing fingerprint.
- Define backup exclusion rules covering authentication tokens and personal data.
- Deploy a consent-management gate for Facebook SDK behavioral tracking.

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. 6, 13, 25, 32, 46. REF DROETKER-2026-R1.