Coordinated Privacy Disclosure, Final Report

Meine Allianz Android (at.aztec.customer)

Allianz Elementar Versicherungs-AG, Austria; platform built by aztec GmbH

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE STATED 19 SEPTEMBER EMBARGO, FIVE MESSAGES, TWO AUTOMATED FMA-DEFLECT ACKNOWLEDGMENTS, ZERO SUBSTANTIVE REPLY

Target	Meine Allianz, the customer app for Allianz Elementar Versicherungs-AG
Package	at.aztec.customer, version 2.8.4, built on the aztec GmbH platform
Operator	Allianz Elementar Versicherungs-AG (data controller), aztec GmbH (data processor, Art. 28 GDPR)
Initial Disclosure	2026-06-26
Stated Embargo	2026-09-19, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, six days after the stated date
Regulators	Austrian DSB, Austrian FMA, EDPS
Total Outbound Messages	5, across 72 days, to datenschutz@allianz.at, presse@allianz.at, and kundenportal@allianz.at.
Inbound Replies	2 automated deflection replies from the Austrian FMA's general feedback address, redirecting to standard consumer channels, not from Allianz itself. No reply of any kind was ever received from Allianz or aztec.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 26 June 2026, RFI-IRFOS disclosed to Allianz Elementar Versicherungs-AG and aztec GmbH, the platform provider building the Meine Allianz app, that the production binary's TLS certificate validation is completely disabled. The method responsible, checkServerTrusted(), contains no code and returns immediately; the accompanying HostnameVerifier returns a hardcoded true for every hostname. Both are extracted verbatim from the production APK, publicly available on Google Play. RFI-IRFOS holds this finding at CRITICAL under an explicit blast-radius escalation beyond its computed HIGH/8.6 band: any attacker sharing a network with a Meine Allianz customer, a café, a hotel, an airport, a public charging station, can intercept the app's full traffic in real time, including login credentials, policy documents, claim submissions with attached photos, and payment methods, with no special hardware required.

A second finding compounds the first directly: cleartext traffic is explicitly enabled (usesCleartextTraffic="true"), and no network security configuration file exists in the APK at all, no domain restrictions, no cleartext blocking, no certificate pinning. Combined with the empty certificate validation, the app has zero functional TLS protection of any kind for its traffic to portal.allianz.at. RFI-IRFOS holds this finding at the same CRITICAL level for the identical reason: together, the two findings describe one fully exploitable, trivial interception path against a live financial application.

Two further findings round out the disclosure: five internal staging, test, and development environment URLs, spanning four distinct environment names, along with the internal Adobe CMS project identifier, are hardcoded in the production JavaScript bundle shipped to every device that has ever installed the app, a direct attack-surface map against Allianz's internal infrastructure if those environments carry weaker security than production; and Android backup is enabled with no exclusion rules, meaning insurance policy documents, claim submissions and photos, payment methods, biometric session tokens, and correspondence history are all subject to Google Cloud Backup, restoring automatically to any Google account signed into a device that later receives them. Genuine positives are worth naming: the app carries no pre-consent tracking SDKs, requests minimal permissions, and Allianz Austria was the first Austrian insurer to receive EuroPrivacy certification under GDPR Art. 42. The certificate validation failure has every appearance of an unreviewed platform-level default in the aztec build environment, not a deliberate decision, which is exactly why a fast, clean fix was available and was never taken.

Five messages were sent across 72 days, to datenschutz@allianz.at, presse@allianz.at, and kundenportal@allianz.at, cc'ing the Austrian DSB, the Austrian FMA, and the EDPS throughout. Two replies arrived, both automated deflection responses from the FMA's general consumer-feedback address redirecting inquiries to standard channels, not from Allianz or aztec, and not addressing a single finding. No reply of any kind was ever received from either the controller or the processor. The 90-day embargo, stated directly to the target in the initial disclosure, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Meine Allianz Android application (at.aztec.customer, version 2.8.4), pulled from Google Play and reviewed on 26 June 2026, including full smali-level decompilation of the certificate validation and hostname verification classes. No man-in-the-middle attack was actively performed against production traffic; the finding is based entirely on static analysis of the shipped binary's own validation code.

Disposition

Four findings were disclosed on 26 June 2026, re-scored under CVSS v4.0. Completely disabled TLS certificate validation, an empty checkServerTrusted() method accepting any certificate including attacker-generated ones, reaches HIGH/8.6 on its own computed band and is held at CRITICAL under an explicit RFI-IRFOS blast-radius escalation: this is a trivially exploitable man-in-the-middle vector on any shared network, café, hotel, airport, requiring no special hardware, against a live production insurance app handling login credentials, claim submissions, and payment methods. Explicitly enabled cleartext traffic with no network security configuration, compounding C1 into zero functional TLS protection, is held at the same level for the same reason. Hardcoded internal staging and CMS infrastructure corrects to MEDIUM. Android backup enabled with no exclusion rules over insurance policy, claims, and payment data corrects to HIGH on its own computed band. Five messages were sent across 72 days. The only inbound replies were two automated deflection acknowledgments from the Austrian FMA's general feedback address, not from Allianz. No reply of any kind was ever received from Allianz or aztec.

ID	Severity	Title
C1	CRITICAL	TLS Certificate Validation Completely Disabled in Production
C2	CRITICAL	Cleartext Traffic Explicitly Enabled, No Network Security Configuration
H1	MEDIUM	Internal Staging and Test Infrastructure Hardcoded in the Production Binary
M1	HIGH	Android Backup Enabled With No Exclusion Rules Over Insurance and Payment Data

Subject & Operator Analysis

Meine Allianz is Allianz Elementar Versicherungs-AG's Austrian customer app, built on the aztec GmbH platform under the package identifier at.aztec.customer, aztec's generic customer-app identifier, not an Allianz-specific binary name. Allianz Elementar is the GDPR data controller; aztec GmbH is the data processor under Art. 28. RFI-IRFOS disclosed to both simultaneously.

Genuine positives are worth naming. Meine Allianz contains no pre-consent tracking SDKs, no Firebase InitProvider, no Facebook AppEvents, no advertising SDK auto-initialization before user interaction. The app requests minimal permissions, no background location, contacts, or calendar. Allianz Austria was the first Austrian insurer to receive EuroPrivacy certification under GDPR Art. 42, which shows real compliance investment at the policy level. The certificate validation failure has every appearance of an unreviewed platform-level default in the aztec build environment, not a deliberate decision, which is exactly why the fix path is fast and clean: a single plugin configuration change and two manifest lines.

Five Messages, Two FMA Auto-Deflects, Zero Substantive Reply

All five messages in this case's correspondence record were delivered to datenschutz@allianz.at, presse@allianz.at, and kundenportal@allianz.at across 72 days, cc'ing the Austrian DSB, the Austrian FMA, and the EDPS throughout. Two replies arrived from FMA-feedback@fma.gv.at, both automated redirections to the FMA's standard consumer-inquiry channels, not from Allianz or aztec, and not addressing a single one of the four findings. No reply of any kind was ever received from either the data controller or the data processor.

Findings

C1: TLS Certificate Validation Completely Disabled in Production

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.

CordovaServerTrust$1.smali implements X509TrustManager's checkServerTrusted() as an empty method that returns immediately, accepting every certificate presented, self-signed, expired, revoked, or attacker-generated. The accompanying HostnameVerifier in CordovaServerTrust$2.smali returns a hardcoded true for every hostname. Both are extracted verbatim from the production APK. RFI-IRFOS blast-radius escalation: raised from HIGH/8.6 to CRITICAL because this is a trivially exploitable man-in-the-middle vector on any shared network, requiring no special hardware, against a live insurance app handling login credentials, claim submissions with photos, and payment methods.

```
checkServerTrusted([X509Certificate;String)V: empty, return-void (accepts all certs)
HostnameVerifier.verify(String, SSLSession)Z: const/4 p1, 0x1 (hardcoded true, all
    hosts)
```

Impact: Any attacker sharing a network with a Meine Allianz customer, a cafe, a hotel, an airport, a public charging station, intercepts the app's full traffic in real time, no special hardware required, exposing login credentials, policy documents, claim submissions, and payment methods.

Fix: Set the Cordova SSL plugin's mode to normal in production and remove the empty trust manager and hostname verifier overrides. No confirmation that this has occurred was ever received.

C2: Cleartext Traffic Explicitly Enabled, No Network Security Configuration

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 is explicitly set to true, and no network_security_config.xml is present in the APK at all: no domain restrictions, no cleartext blocking, no certificate pinning. Combined with C1's empty certificate validation, the app has zero functional TLS protection for its traffic to portal.allianz.at. RFI-IRFOS blast-radius escalation: held at CRITICAL for the same reason as C1, together the two findings describe one fully exploitable, trivial interception path against a live financial application.

```
android:usesCleartextTraffic="true"
res/xml/network_security_config.xml: not present in APK
```

Impact: With cleartext explicitly permitted and no certificate validation in place, all traffic between Meine Allianz and Allianz's own servers is fully exposed on any shared network.

Fix: Add a network security config with cleartextTrafficPermitted="false". No confirmation that this has occurred was ever received.

H1: Internal Staging and Test Infrastructure Hardcoded in the Production Binary

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.

Five distinct staging, test, and development environment URLs, spanning dev, hot, test, and stg1 environment names, along with the internal Adobe CMS project identifier (azat), are hardcoded in the production JavaScript bundle shipped to every device that has ever installed the app.

```
allianz-emea-stg1.adobecqms.net/.../azat/dev-allianz-at/... (and 4 further internal
    environment URLs)
secure-test.allianz.at/os-motor, /os-property
Internal Adobe CMS project identifier: azat
```

Impact: If these non-production environments carry a weaker security posture than production, different authentication, older software, reduced monitoring, this URL map is a direct attack-surface enumeration against Allianz's internal systems.

Fix: Remove all non-production environment references from the production build. No confirmation that this has occurred was ever received.

M1: Android Backup Enabled With No Exclusion Rules Over Insurance and Payment 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.

android:allowBackup is set to true with neither backup_rules.xml nor data_extraction_rules.xml present. Insurance policy documents, FNOL claim submissions and photos, payment methods, biometric session tokens, correspondence history, and policy and contract numbers are all subject to Android Cloud Backup.

```
android:allowBackup="true"
res/xml/backup_rules.xml: not present
res/xml/data_extraction_rules.xml: not present
```

Impact: On a stolen device with a freshly signed-in Google account, all locally stored insurance data, policy documents, claims with photos, and payment methods, restores automatically with no exclusion in place.

Fix: Define explicit backup exclusion rules covering all sensitive local data categories. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR and NIS2 provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 32, Art. 5(1)(f), NIS2 Art. 21	C1	Completely disabled TLS certificate validation.
Art. 32, Art. 5(1)(f)	C2	Explicitly enabled clear-text traffic, no network security configuration.
Art. 32	H1	Internal staging and CMS infrastructure hardcoded in production.
Art. 32, Art. 5(1)(f)	M1	Unrestricted Android backup over insurance and payment 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 CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own. In this report, C1 and C2 are held at CRITICAL under an explicit, stated blast-radius escalation beyond their computed HIGH/8.6 band. M1 corrects to HIGH and H1 corrects to MEDIUM, both on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: #AZTEC-2026-001.