



Security & Privacy Disclosure, Final Report

Müller App (at.helloagain.muellerde), Android

A drugstore loyalty and payment-adjacent app shipped with app-wide cleartext HTTP permitted, a broad permission set and two unrotated Google API keys; the operator answered five times in substance, removed cleartext HTTP and the overlay permission within about ten weeks, and a first reading of the SDK stack was retracted by RFI-IRFOS where the operator proved it wrong

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 29
SEPTEMBER 2026, FIVE SUBSTANTIVE REPLIES, TWO FIXES VERIFIED, ONE
FINDING PART RETRACTED, FOUR OPERATOR STATEMENTS NOT VERIFIABLE
FROM THE BINARY**

Target	Müller App, operator correspondence signed by Müller Holding GmbH & Co. KG, Albstraße 92, 89081 Ulm-Jungingen; app platform provider hello again GmbH
Package	at.helloagain.muellerde
Versions Analysed	2.19.0 (versionCode 197) for the original disclosure; 2.21.0 for the independent verification of 11 September 2026
Platform Audited	Android, static root level code analysis of the production APK (manifest, resources, classes*.dex). No live traffic capture, no dynamic instrumentation, no probing of Müller or hello again systems
Initial Disclosure (R1)	2026-07-01, to datenschutz@mueller.de and privacy@helloagain.at, with the supervisory authorities LfDI Baden-Württemberg, EDPS and the Austrian Datenschutzbehörde on the same message
Disclosure / Embargo Date	2026-09-29
Report Published	2026-10-17
Overall Severity	HIGH (H-1, now fixed)
Findings	6 (1 High, 4 Medium, 1 Low). H-2 and H-3 were rated HIGH in the R1 and are re-rated MEDIUM in this report, reasons stated in the findings
Correspondence	8 messages sent by RFI-IRFOS over 82 days (2026-07-01 to 2026-09-21); 5 substantive replies from the operator (2026-07-30, 2026-08-10, 2026-09-11, 2026-09-16, 2026-09-21), 3 automatic ticket acknowledgements, 6 automatic acknowledgements from LfDI Baden-Württemberg; no message from the operator after 2026-09-21
Authorities Notified	LfDI Baden-Württemberg · Austrian Datenschutzbehörde (dsb@dsb.gv.at) · European Data Protection Supervisor (edps@edps.europa.eu)
SHA-256 (base APK)	v2.19.0 base.apk b4a184d91f1fd506dac76b3f5c268815d38f8b97f4b8fe13a9193685e221d9f0 · v2.21.0 base.apk 302946d9d255ec6b5f0b8eada945680db8e87d017738b1d79b523c6417c31ba9

security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Architecture & Data Flow	5
4	Findings	6
4.1	H-1: App-wide cleartext HTTP permitted on a loyalty and payment-adjacent client (FIXED in 2.21.0)	6
4.2	H-2: Loyalty purchase profiling alongside Adjust and Facebook SDKs on health-inferable drugstore purchases (AppsFlyer part retracted, remainder an inference)	7
4.3	H-3: Permission set broader than a loyalty app needs (SYSTEM_ALERT_WINDOW removed, rest justified by the operator)	8
4.4	M-1: Two extractable Google API keys unchanged between 2.19.0 and 2.21.0, with Realtime Database and Storage bucket references in the configuration . .	9
4.5	M-2: Sentry, Firebase and Crashlytics telemetry started by ContentProviders at process start	10
4.6	L-1: Third-party components initialise through ContentProviders before any consent screen	10
5	Impact Analysis	11
6	The Complete Chain: From Install to Residual Exposure	11
7	Data Protection – Article by Article	12
8	Regulatory & Legal Landscape	12
9	Indicators of Compromise & Reproducible Evidence	13
10	Disclosure Timeline & Outcome	13
11	Residual Risk & Recommendations	14

Executive Summary

The Müller App is the loyalty and coupon app of the German drugstore chain Müller, built on the Austrian hello again loyalty platform and carrying the Bluecode mobile-payment SDK. A static analysis of version 2.19.0 on 1 July 2026 produced six findings: app-wide cleartext HTTP permitted without any network security configuration (H-1), a loyalty purchase-profiling stack alongside Adjust and Facebook SDKs over health-inferable drugstore purchases (H-2), a permission set broader than a loyalty app needs (H-3), two extractable Google API keys (M-1), overlapping crash and telemetry pipelines (M-2) and several components that initialise before any consent screen (L-1).

This case is a documented example of a coordinated disclosure that mostly worked. Müller answered five times in substance. Between 10 August and 11 September 2026 the operator removed the global cleartext flag and the SYSTEM_ALERT_WINDOW permission, and RFI-IRFOS verified both against version 2.21.0 on a physical device. Müller also proved one sub-claim of H-2 wrong: the AppsFlyer references in the binary are an inactive Usercentrics consent-mediation adapter, not an integration. RFI-IRFOS retracted that part of H-2 in writing on 11 September 2026, the same day the proof arrived.

Four points stay with the operator's word because a client-side binary cannot settle them: the consent gate in front of Adjust, the Facebook SDK being used for login only, the server-side restrictions on the two Google API keys together with the state of the Realtime Database named in the Firebase configuration, and a threshold analysis for fine location, clipboard and calendar access that Müller confirmed exists but did not date or share. RFI-IRFOS records each statement as Müller's statement and does not present any of them as verified.

The embargo date of 29 September 2026 passed without a further message from either side after 21 September 2026. This report publishes 18 days after the embargo and 108 days after the original disclosure. It replaces the earlier ledger wording on H-2: the link between drugstore purchase categories and the Adjust and Facebook SDKs was an inference from their shared presence in the binary from the first message on, and the ledger text that stated it as an observed transfer was corrected on 21 September 2026.

ID	Severity	Title
H-1	HIGH	App-wide cleartext HTTP permitted on a loyalty and payment-adjacent client (FIXED in 2.21.0)
H-2	MEDIUM	Loyalty purchase profiling alongside Adjust and Facebook SDKs on health-inferable drugstore purchases (AppsFlyer part retracted, remainder an inference)
H-3	MEDIUM	Permission set broader than a loyalty app needs (SYSTEM_ALERT_WINDOW removed, rest justified by the operator)
M-1	MEDIUM	Two extractable Google API keys unchanged between 2.19.0 and 2.21.0, with Realtime Database and Storage bucket references in the configuration
M-2	MEDIUM	Sentry, Firebase and Crashlytics telemetry started by ContentProviders at process start
L-1	LOW	Third-party components initialise through ContentProviders before any consent screen

Subject & Operator Context

The Müller App is published for Android as `at.helloagain.muellerde`. The correspondence was answered by the Müller data protection team (Müller Holding GmbH & Co. KG, Albstraße 92, 89081 Ulm-Jungingen, registered at the Amtsgericht Ulm under HRA 720465) through the mailbox `privacy@ds.de.mueller.eu`, a Zendesk-based ticket system. Müller named hello again GmbH as its app provider and processor, and referred to a data processing agreement under Art. 28 GDPR with it. The original R1 named Müller Handels GmbH as the retail brand entity. Because the Ulm seat signs the data protection correspondence, the Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) was added as recipient from the first message, together with the Austrian Datenschutzbehörde (hello again is Austria-based) and the EDPS.

The app is a React Native application on the hello again platform. The package contains the classes `com.helloagain.FrederixConnect` and `com.seblau.helloagain`, the Usercentrics consent management platform, Adjust, the Facebook SDK, Firebase with Crashlytics references, Sentry, Google ML Kit barcode scanning and the Bluecode payment SDK (`at.bluecode.sdk`).

Architecture & Data Flow

From the manifest and resources of version 2.19.0 (original disclosure) and 2.21.0 (verification):

Process start: six ContentProviders run before any screen renders (`FacebookInitProvider`, `FirebaseInitProvider`, `ReactNativeFirebaseAppInitProvider`, `SentryInitProvider`, the Bluecode `Initializer`, `MIKitInitProvider`). Whether they transmit anything before consent depends on runtime configuration and is not settled by the binary.

Consent layer: Usercentrics is present. In version 2.21.0 Adjust is no longer started from a ContentProvider but through an exposed React Native bridge method (`com/adjust/nativemodule/Adjust initSdk`). The JavaScript that decides when that method runs is Hermes-compiled bytecode that RFI-IRFOS cannot disassemble, so the consent gate Müller describes is plausible and unverified.

Identity and payments: loyalty account, coupon and card data sit on the hello again platform. Bluecode handles in-store mobile payment, with biometric release (`USE_BIOMETRIC`, `USE_FINGERPRINT`).

Google services: the Firebase project is `mueller-de`. Version 2.21.0 still carries `google_api_key`, `google_app_id`, the Maps key in the manifest, `firebase_database_url` (`mueller-de.firebaseio.com`) and `google_storage_bucket` (`mueller-de.appspot.com`). Firebase App Check with a Play Integrity provider and a custom provider factory (`com/seblau/safety net/playintegrity`) is configured, which is a genuine positive.

Findings

H-1: App-wide cleartext HTTP permitted on a loyalty and payment-adjacent client (FIXED in 2.21.0)

MEDIUM, CVSS v4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 6.0 — flag removed in the operator's release of early September 2026, verified

```
v2.19.0: android:usesCleartextTraffic="true"    (no networkSecurityConfig, no res/xml
        NSC file)
v2.21.0: android:usesCleartextTraffic="false"
Mueller statement 2026-07-30: flag kept for WebView resources; API traffic HTTPS
Mueller statement 2026-09-11: cleartext support globally disabled in the September
        release
```

Status: FIXED and verified. Time from disclosure to verified fix: 72 days (2026-07-01 to 2026-09-11, fix announced for early September).

Impact: RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because the flag applied to every network request of every installed copy, on a client that also carries account, coupon and payment-adjacent traffic, and because Müller stated on 30 July 2026 that the flag had been left set deliberately for WebView resources rather than by oversight. The CVSS vector scores only the capability, not the operator's deliberate choice. Version 2.19.0 declared `android:usesCleartextTraffic="true"` in the manifest with no `networkSecurityConfig`, so the operating system allowed unencrypted HTTP for every host the app contacted. An attacker on the same network path as a user could read or alter any request that an endpoint served over HTTP. Müller stated that all hello again API requests use HTTPS and that a penetration test had found the flag uncritical, and that only WebView resources such as shop images could use HTTP. The binary alone does not show which endpoints used HTTP. The flag was deactivated in version 2.21.0 (`usesCleartextTraffic="false"`), independently verified by RFI-IRFOS on 11 September 2026. Remaining exposure for users who have not updated: none that RFI-IRFOS can quantify.

H-2: Loyalty purchase profiling alongside Adjust and Facebook SDKs on health-inferable drugstore purchases (AppsFlyer part retracted, remainder an inference)

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 — re-rated from HIGH after the AppsFlyer retraction and the operator's consent-gate statement

RFI-IRFOS re-rating: the R1 rated this finding HIGH. After the AppsFlyer retraction below and Müller's statements on consent gating and data scope, the finding rests on an unverified inference, so this report rates it MEDIUM.

```
Only reference: com/usercentrics/sdk/mediation/sdk/AppsFlyerMediationSDK.smali
Method performs Class.forName("com.appsflyer.AppsFlyerLib") inside try/catch
No com/appsflyer/* classes exist in any classes*.dex
Result: ClassNotFoundException is caught, no data flow possible
Crashlytics shows the same pattern (CrashlyticsMediationSDK.smali stub only)
```

```
com/adjust/nativemodule/Adjust -> initSdk exposed as React Native bridge method
No ContentProvider auto-init for Adjust (improved against 2.19.0)
Consent gate logic lives in Hermes bytecode: not readable, claim unverified
```

Müller's statement (2026-07-30, 2026-08-10, 2026-09-11, 2026-09-21): the Facebook SDK serves login only, with `AutoLogAppEventsEnabled=false`, `AdvertiserIDCollectionEnabled=false`, `AutoInitEnabled=false` and `firebase_analytics_collection_enabled=false` set in the manifest. RFI-IRFOS recorded these as Müller's statement and did not independently verify the flags in this report.

Impact: A drugstore loyalty platform builds purchase profiles by design, and drugstore purchase categories such as medication, pregnancy tests or baby and care products allow inferences about health. The binary contains the hello again loyalty platform next to the Adjust SDK (attribution and analytics endpoints) and the Facebook SDK. RFI-IRFOS documented the link between purchase categories and these SDKs from the first message as an inference from their shared presence in the binary and never as an observed transfer of purchase data. Müller states that no product, basket or category data goes to Adjust or Facebook and that Adjust runs only after consent through Usercentrics (Art. 6(1)(a) GDPR). RFI-IRFOS did not capture traffic and does not claim a transfer.

H-3: Permission set broader than a loyalty app needs (SYSTEM_ALERT_WINDOW removed, rest justified by the operator)

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 — re-rated from HIGH after removal of the overlay permission and documented purposes

RFI-IRFOS re-rating: the R1 rated this finding HIGH on the breadth of the set. Müller documented a purpose per permission, removed the one with the highest risk and confirmed a threshold analysis (see below), so the remaining finding is a minimisation question and is rated MEDIUM here.

Open point: on 21 September 2026 Müller confirmed in writing that its data protection team carried out a documented threshold analysis for fine location, clipboard and calendar access, and that no DPIA under Art. 35 GDPR was required. The date of that analysis was requested on 21 September 2026 and was not provided. Müller declined on 16 September to hand out internal documentation, which RFI-IRFOS accepts. The statement stands as Müller's statement.

Impact: Version 2.19.0 declared CAMERA, ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION, READ_CLIPBOARD and WRITE_CLIPBOARD, READ_CALENDAR and WRITE_CALENDAR, SYSTEM_ALERT_WINDOW, USE_BIOMETRIC and USE_FINGERPRINT, RECEIVE_BOOT_COMPLETED and the Google AD_ID permission. Müller gave a functional purpose for each: QR and barcode scanning for cards and coupons, store finder, copying codes from deep links for a friend-invite feature, an events extension that writes appointments to the calendar, biometric release for Bluecode payments, and consent-based attribution for AD_ID. SYSTEM_ALERT_WINDOW was announced for removal on 10 August and is absent from the manifest of 2.21.0, verified on 11 September 2026.

M-1: Two extractable Google API keys unchanged between 2.19.0 and 2.21.0, with Real-time Database and Storage bucket references in the configuration

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9 — availability and billing exposure; protective restrictions claimed by the operator, not verifiable client-side

```
google_api_key      ...AIzaSyBlCA  (identical in 2.19.0 and 2.21.0)
google_app_id       1:1081381974475:android:171adc4df1a408484fc64e
project_id          mueller-de
com.google.android.geo.API_KEY  ...AIzaSyDrRG  (identical in 2.19.0 and 2.21.0)
firebase_database_url  https://mueller-de.firebaseio.com  (present in 2.21.0)
google_storage_bucket  mueller-de.appspot.com            (present in 2.21.0)
Firebase Auth module bundled; App Check: PlayIntegrityAppCheckProviderFactory + custom
factory
```

Status: UNVERIFIED by RFI-IRFOS. Müller's statement of 21 September 2026 answers the question RFI-IRFOS asked (which restrictions are active), and a keyless client binary cannot confirm it. The shared Maps key without an app restriction is an operator-stated, separate residual point.

Impact: The Firebase API key (google_api_key, project mueller-de) and the Google Maps key in the manifest are byte-identical in 2.19.0 and 2.21.0. Müller announced on 10 August 2026 that unused services of both keys would be disabled by early September, and on 21 September 2026 named the services enabled on its own key (Maps SDK for Android, Places API, Geocoding API, Directions API) plus a restriction to the official package and production SHA-1 certificate fingerprint. For the Maps key Müller stated that it is shared by hello again across several apps and carries no app-specific restriction, with the same four APIs enabled. Version 2.21.0 also still contains firebase_database_url and google_storage_bucket. Müller stated that the Realtime Database was never activated, is deny-by-default and that the entry is a dead remnant that Google does not allow removing. RFI-IRFOS cannot check server-side restrictions or database state without live probing, which this programme does not do.

M-2: Sentry, Firebase and Crashlytics telemetry started by ContentProviders at process start

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 — overlapping telemetry pipelines; transmission before consent not shown

```
io.sentry.android.core.SentryInitProvider
com.google.firebase.provider.FirebaseInitProvider
io.invertase.firebase.app.ReactNativeFirebaseAppInitProvider
```

Impact: Version 2.19.0 registers `io.sentry.android.core.SentryInitProvider`, `com.google.firebase.provider.FirebaseInitProvider` and `io.invertase.firebase.app.ReactNativeFirebaseAppInitProvider`, which start at process start and give three overlapping crash and telemetry pipelines. In 2.21.0 Crashlytics is reduced to an inactive Usercentrics mediation stub, which lowers the overlap to Sentry plus Firebase. Müller stated that `firebase_analytics_collection_enabled` is false. Whether Sentry or Firebase sends data before a consent decision depends on runtime configuration that the binary does not settle.

L-1: Third-party components initialise through ContentProviders before any consent screen

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 — initialisation is not transmission; Usercentrics gating unverified

```
com.facebook.internal.FacebookInitProvider
com.google.firebase.provider.FirebaseInitProvider
io.sentry.android.core.SentryInitProvider
at.bluecode.sdk.bluecodesdk.Initializer
com.google.mlkit.common.internal.MlKitInitProvider
io.invertase.firebase.app.ReactNativeFirebaseAppInitProvider
```

Impact: `FacebookInitProvider`, `FirebaseInitProvider`, `SentryInitProvider`, the Bluecode Initializer, `MlKitInitProvider` and `ReactNativeFirebaseAppInitProvider` are declared as ContentProviders and run before the first screen. A consent management platform (Usercentrics) is present. Initialisation before consent is a design signal; unlawful processing before consent requires a transmission, which RFI-IRFOS did not capture. Müller states that the Facebook auto-initialisation switches are off.

Impact Analysis

Who is affected: customers of a drugstore chain who use the app for coupons, loyalty points, store search and in-store payment. Purchase data in this sector is more sensitive than in most retail, because categories reveal health-related facts without being formal medical data. That is why the profile question in H-2 carries weight even where no transfer is demonstrated.

What the evidence supports: a deliberate app-wide cleartext setting that the operator removed (H-1), a permission set that the operator explained and trimmed (H-3), and a consent architecture that looks sound on paper and that a client-side review cannot confirm (H-2, M-2, L-1). The residual weight sits with M-1: two keys that were publicly extractable and unchanged after the operator's own announcement, now covered by operator statements about server-side restrictions.

What the evidence does not support: any claim that purchase data reached Adjust or Facebook, any claim that AppsFlyer is integrated, and any claim that the Realtime Database is open. RFI-IRFOS makes none of these claims.

The Complete Chain: From Install to Residual Exposure

Step 1, install: a customer installs the app, and every installed copy carries the same binary, including the same Firebase and Maps keys and, in version 2.19.0, the cleartext permission.

Step 2, process start: six ContentProviders start before any screen (L-1), among them Sentry, Firebase and Facebook components (M-2). The Usercentrics banner then asks for consent. The binary shows that Adjust is no longer started automatically in 2.21.0; the gate itself runs in Hermes bytecode and stays unverified (H-2).

Step 3, use: the customer scans cards and coupons with the camera, searches stores with location, copies invite codes through the clipboard, saves events to the calendar and pays through Bluecode with biometrics (H-3). Each purpose was named by Müller.

Step 4, transport: in 2.19.0 the operating system allowed HTTP for every host (H-1). Müller stated that API traffic ran over HTTPS and removed the flag in the September release.

Step 5, cloud: the keys in the binary identify the Firebase project mueller-de. Müller stated that its restrictions and its disabled Realtime Database keep abuse in check (M-1).

Step 6, correction: Müller's evidence on AppsFlyer ended one strand of the original reading, and RFI-IRFOS retracted it the same day. One further correction followed on 21 September 2026: the public ledger wording had stated the Adjust and Facebook link as fact, and RFI-IRFOS changed it to the inference it always was.

Data Protection – Article by Article

Art. 32(1)(b) GDPR, security of processing: H-1 (cleartext permitted, fixed) and M-1 (publicly extractable keys, restrictions stated by the operator).

Art. 5(1)(f) GDPR, integrity and confidentiality: H-1.

Art. 5(1)(b) and Art. 6(1)(a) GDPR, purpose limitation and consent: H-2. The operator relies on consent via Usercentrics for Adjust. The consent chain (consent string, timestamp, first network call) was requested on 2 September 2026 and answered on 11 September 2026 as an opt-in statement without the artefacts; RFI-IRFOS recorded it as a statement.

Art. 9 GDPR, special categories: H-2 raises it only as an inference risk. The operator states that no product or category data reaches the SDKs, so Art. 9 processing is not shown.

Art. 5(1)(c) GDPR, data minimisation: H-3.

Art. 35 GDPR, data protection impact assessment: H-3. Müller states that a threshold analysis concluded that no DPIA was required. Date and author team were requested; the team (data protection team of Müller Holding GmbH & Co. KG) was named, the date was not.

Art. 7 and Art. 13 GDPR, conditions for consent and information duties: M-2 and L-1, as design signals without demonstrated transmission.

Art. 33(4) GDPR was cited in correspondence as a note on staged reporting. RFI-IRFOS does not assert that a notifiable breach occurred.

Regulatory & Legal Landscape

The data protection supervisory authority for the Ulm seat is the LfDI Baden-Württemberg, which acknowledged each message automatically; the Austrian Datenschutzbehörde and the EDPS were also on the correspondence. No authority wrote back.

Two procedural points from the correspondence. First, on 10 August 2026 Müller asked that authorities no longer be copied. RFI-IRFOS declined: copying the competent authorities is part of the disclosure procedure that applied from the first message of 1 July 2026. Müller then explained the missing authority copies in its replies first as a technical limit of its ticket system and later (21 September 2026) as a deliberate administrative setting of its Zendesk instance. RFI-IRFOS recorded both explanations in sequence. Second, Müller reserved legal steps over alleged false statements of fact on this website and asked for removal from the ledger. RFI-IRFOS asked twice for the single finding it considers factually wrong. Müller named only the AppsFlyer reading, and RFI-IRFOS retracted it. No other finding was named as incorrect.

Fine exposure under the GDPR for the issues in H-1 and M-1 falls under Art. 83(4), up to EUR 10,000,000 or 2% of total worldwide annual turnover; Art. 83(5) covers the consent and minimisation questions in H-2, H-3, M-2 and L-1, up to EUR 20,000,000 or 4%. These ceilings describe the legal frame and are not a prediction. Research is conducted under ISO/IEC 29147, Art. 17 StGG (freedom of science) and GDPR Art. 89.

Indicators of Compromise & Reproducible Evidence

All evidence comes from static analysis of the published APK. No Müller or hello again server, account or infrastructure was probed. API key values are truncated in this public report; full values were sent privately to the operator in the R1.

```
Package                at.helloagain.muellerde
v2.19.0 base.apk      SHA-256
                        b4a184d91f1fd506dac76b3f5c268815d38f8b97f4b8fe13a9193685e221d9f0
v2.21.0 base.apk      SHA-256 302946
                        d9d255ec6b5f0b8ead945680db8e87d017738b1d79b523c6417c31ba9
Firebase project       mueller-de
Firebase app id        1:1081381974475:android:171adc4df1a408484fc64e
Endpoints in cfg       mueller-de.firebaseio.com, mueller-de.appspot.com
Attribution           app.adjust.com, gdpr.adjust.com, ssrv.adjust.com, subscription.
                        adjust.com
Mediation stubs        com/usercentrics/sdk/mediation/sdk/AppsFlyerMediationSDK,
                        CrashlyticsMediationSDK
Payment SDK            at.bluecode.sdk.bluecodesdk
Tools                  apktool (manifest, resources), classes*.dex string analysis
```

Disclosure Timeline & Outcome

2026-07-01 R1 sent to datenschutz@mueller.de and privacy@helloagain.at, with LfDI Baden-Württemberg, EDPS and the Austrian Datenschutzbehörde on the message. Embargo stated as 2026-09-29. Automatic ticket acknowledgement from privacy@ds.de.mueller.eu the same minute.

2026-07-23 First follow-up, 23 days after the R1. Automatic acknowledgement from LfDI Baden-Württemberg.

2026-07-30 First substantive reply from Müller (data protection team): statement on each finding, announced review of the API-key services without date. RFI-IRFOS answered the same day.

2026-08-10 Second substantive reply: no data protection violation, three dated measures announced for early September (cleartext HTTP, SYSTEM_ALERT_WINDOW, unused API-key services), AppsFlyer reference described as inactive Usercentrics code, request that authorities not be copied, reservation of legal steps. RFI-IRFOS answered the same day with five questions.

2026-09-02 RFI-IRFOS message after the announced early-September date, asking for confirmation with version number. Automatic acknowledgement.

2026-09-11 Third substantive reply: hardening measures reported as implemented, five questions answered, request for removal from the website. RFI-IRFOS verified version 2.21.0 on a physical device the same day and replied: H-1 fixed, SYSTEM_ALERT_WINDOW removed, AppsFlyer retracted, keys unchanged, four points open with a deadline of 18 September.

2026-09-16 Fourth reply: statements on key rotation, Realtime Database, internal documentation, Zendesk, and questions about RFI-IRFOS's assignment and the service tiers mentioned in the R1. RFI-IRFOS replied the same day: the programme runs without assignment,

disclosure is unconditional and free, no payment influences whether or when a finding is published.

2026-09-21 Fifth reply: restrictions of the Google API keys, Realtime Database described as dead remnant, threshold analysis confirmed, CC setting described as deliberate administrative choice. RFI-IRFOS replied the same day: three points progressed, ledger wording on H-2 corrected, threshold analysis date still open.

2026-09-29 Embargo date reached. No message from either side.

2026-10-17 This report published, 18 days after the embargo and 26 days after the last message. Record: eight messages sent by RFI-IRFOS, five substantive replies from Müller, three automatic ticket acknowledgements, six automatic acknowledgements from LfDI Baden-Württemberg, no bounce.

Residual Risk & Recommendations

H-1: done. Keep `usesCleartextTraffic` false and add an explicit network security configuration that names the hosts, so that a later `WebView` change cannot silently reopen it.

H-2: publish the consent artefacts for Adjust (consent string, timestamp, first network call) to the data protection officer's file, and keep the Facebook switches off in the manifest. A reproducible test of the opt-out path is the only thing that closes this finding.

H-3: add the date and the author team of the threshold analysis to the processing records so that it can be produced to a supervisory authority on request. Re-assess the clipboard permissions, since both read and write access exist.

M-1: confirm in the Google Cloud console that the Firebase key carries the package and SHA-1 restriction and only the four named APIs, and split the Maps key so that it no longer serves several apps without an app restriction. Remove the Realtime Database URL from the Firebase configuration if the project permits it.

M-2 and L-1: keep Sentry and Firebase collection off until the consent decision, and document it.

RFI-IRFOS remains open to a substantive answer on any open point in this thread at any time. Such an answer will be added to the public record next to the original findings, whichever entity it comes from.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of the published application using publicly available tooling. No Müller or hello again server, account or infrastructure was probed and no traffic was captured. API key values are truncated in this public report; full values were disclosed privately in the original R1 letter. Statements by the operator are recorded as statements. Technical evidence is archived under chain of custody. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF MUELLER-2026-R1-001.