



Coordinated Security & Privacy Disclosure, Final Report

Tchibo App for Android (de.tchibo.app, v10.24.0)

Eight written notices across two parallel channels, eighty-nine days, one general denial received the day before embargo, zero point-by-point rebuttal

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – FIVE FINDINGS PUBLISHED, ONE GENERAL DENIAL RECEIVED, NO FINDING SPECIFICALLY REBUTTED

Target	Tchibo GmbH, Ueberseering 18, 22297 Hamburg, Germany
Product audited	Tchibo App for Android, de.tchibo.app, v10.24.0
Disclosure reference	REF TCHIBO-2026-R1 (parallel Austrian-market thread: REF AT-TCHIBO-2026-R1, never answered)
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 ContentSquare session-replay auto-starting on launch and capturing checkout/payment flows, CVSS v4.0 8.7, disputed only in general terms, not specifically rebutted)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1	Executive Summary	3
2	Subject & Operator Analysis	4
3	Findings	4
3.1	C1: Firebase API key hardcoded in the public APK under an internally-named project	4
3.2	C2: ContentSquare session-replay auto-starts on launch, full developer UI in the production build	5
3.3	H1: Google Tag Manager container with 22 tracking tags deployed without Play Store review, hardcoded Adjust token	5
3.4	H2: Emarsys geofencing registers on every device boot, independent of app use	6
3.5	H3: Three overlapping advertising-tracking permissions enabling cross-device profiling	6
4	One Reply, One Day Before Embargo, No Point Specifically Rebutted	7
5	Data Protection, Article by Article	7
6	Disclosure Timeline & Outcome	8
7	Residual Risk & Recommendations	8

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Tchibo Android application and identified two CRITICAL and three HIGH findings: a Firebase API key hardcoded in the public APK under an internally-named project ('hunter'), a ContentSquare session-replay integration (292 smali files) that auto-starts on app launch with no user action, capturing taps, scrolls, and screen state including checkout and payment flows, with developer-activation and settings activities left inside the production binary, a Google Tag Manager container (version 28, container ID GTM-NPB86Z3) carrying 22 tracking tags deployed without Play Store review and a hardcoded Adjust app token as a plaintext constant, an Emarsys (SAP) geofencing integration that registers itself on every device boot independent of whether the app has been opened, and three overlapping advertising-tracking permissions (Privacy Sandbox Topics API, Advertising ID, and legacy GMS AD_ID) combined with the Adjust SDK enabling cross-device profiling.

Across eight written notices spanning two parallel correspondence channels over eighty-nine days, Tchibo's customer service twice misread the disclosure as a business-partnership inquiry rather than a GDPR notice. On 18 September, one day before the embargo, Datenschutz@tchibo.de sent Tchibo's only substantive reply of the case: a general denial stating the findings rested on 'unsubstantiated claims,' expressing irritation at RFI-IRFOS's manner of contact, and requesting that no further unsubstantiated claims be published, while separately confirming that any supervisory-authority inquiry would receive a substantive, well-founded answer. The reply named no specific finding, no file, and no technical basis for its disqualification. RFI-IRFOS replied the same day asking Tchibo to identify which of the four technical findings it considered factually incorrect; no answer followed before the embargo. The parallel Austrian-market thread received no reply at any point.

Scope: Static analysis of the publicly downloaded production Tchibo Android APK (v10.24.0), on an authorized test device, only. No Tchibo account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@tchibo.de, bcc the Austrian Datenschutzbehörde, CERT.at, and Hamburg's data protection authority; a parallel Austrian-market thread was opened 28 July to datenschutz@tchibo.at under REF AT-TCHIBO-2026-R1 and never received any reply. On the German thread, Tchibo's customer service twice misread the disclosure as a business-partnership inquiry (25 August, 15 September), and on 18 September, one day before the embargo, Datenschutz@tchibo.de sent Tchibo's only substantive reply: a general denial characterizing the findings as 'unsubstantiated claims' without naming which finding it disputed or offering any technical rebuttal. RFI-IRFOS replied the same day asking Tchibo to specify which of the four technical findings it considered factually incorrect; no answer followed before the embargo.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the public APK under an internally-named project
C2	CRITICAL	ContentSquare session-replay auto-starts on launch, full developer UI in the production build
H1	HIGH	Google Tag Manager container with 22 tracking tags deployed without Play Store review, hardcoded Adjust token
H2	HIGH	Emarsys geofencing registers on every device boot, independent of app use
H3	HIGH	Three overlapping advertising-tracking permissions enabling cross-device profiling

Subject & Operator Analysis

Tchibo GmbH is headquartered in Hamburg, Germany (Amtsgericht Hamburg HRB 43618). Hamburg's data protection authority is Tchibo's lead supervisory authority under GDPR one-stop-shop rules.

Findings

C1: Firebase API key hardcoded in the public APK under an internally-named project

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 AlzaSyAVbsVK_eN3VmU3qKvt7qwL7Oiuog_yPSU, Firebase project tc h-hunter-mobile-app-live, App ID 1:303533861508:android:d024ac05f8d772fa90f0d1, storage bucket tch-hunter-mobile-app-live.appspot.com.

Tchibo's 18 September reply did not name this finding or dispute it specifically.

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 deny-by-default security rules, and enforce App Check for this project.

C2: ContentSquare session-replay auto-starts on launch, full developer UI in the production build**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**

292 small files (230 Flutter, 62 Android) implement ContentSquare. It auto-initializes on app launch with no user action, and an OverlayService captures taps, scrolls, and screen state, including checkout and payment flows. DeveloperActivationActivity, SettingsActivity, and ClientModeTutorialActivity remain inside the production binary.

Tchibo's 18 September reply did not name this finding or dispute it specifically.

Impact: Checkout and payment-flow interactions may be captured via session replay before any consent decision is made, given the SDK's auto-start behavior, and development-only UI remains reachable in the shipped app.

Fix: Gate ContentSquare initialization behind an affirmative consent decision, exclude checkout/payment screens from capture, and strip developer-activation activities from production builds.

H1: Google Tag Manager container with 22 tracking tags deployed without Play Store review, hardcoded Adjust token**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**

GTM container GTM-NPB86Z3, version 28, carries 22 tags (9 Adjust, 7 __flc, 2 __fls, 1 __sp, 2 paused). The Adjust app token b33ubxkxgrsy is present as a plaintext constant. Server-side tag containers of this kind can add tracking behavior after Play Store review without a new app submission.

Tchibo's 18 September reply did not name this finding or dispute it specifically.

Impact: Tracking behavior can be altered post-review via remote tag configuration, outside the scope of any app-store privacy review process.

Fix: Subject GTM container changes to the same privacy review as app releases, and remove the hardcoded Adjust token.

H2: Emarsys geofencing registers on every device boot, independent of app use

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.emarsys.geofence.RegisterGeofencesOnBootCompletedReceiver, GeofenceBroadcastReceiver, and EmarsysFirebaseMessagingService register GPS geofences active from device boot, independent of whether the app has ever been opened by the user in that session.

Tchibo's 18 September reply did not name this finding or dispute it specifically.

Impact: Location-based geofence monitoring may operate from the moment a device boots, without the app having been actively used, exceeding what an opt-in location feature would suggest.

Fix: Register geofences only after the user has actively opened the app and granted location permission in-session, not automatically on every boot.

H3: Three overlapping advertising-tracking permissions enabling cross-device profiling

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

ACCESS_AD SERVICES_ATTRIBUTION (Privacy Sandbox Topics API), ACCESS_AD SERVICES_AD_ID, and the legacy Google Ad ID overlap, combined with the Adjust SDK (197 small classes) and 9 Adjust tags in the GTM container.

Tchibo's 18 September reply did not name this finding or dispute it specifically.

Impact: Three redundant advertising-identifier mechanisms combined with an active attribution SDK enable cross-device profiling beyond what a single, disclosed mechanism would require.

Fix: Consolidate to a single advertising-identifier mechanism with an explicit consent gate, and disclose the specific combination in use.

One Reply, One Day Before Embargo, No Point Specifically Rebutted

Tchibo's only substantive reply in this case arrived on 18 September, eighty-nine days after R1 and one day before the embargo. In full relevant part: 'Wir halten vorangestellt fest, dass wir ueber die Art und Weise Ihrer Kontaktaufnahmen irritiert sind... die damals hoechst vorsorglich vorgenommene interne Pruefung ergeben hat, dass Sie von unzutreffenden Sachverhaltsannahmen ausgehen. Es handelt sich um unsubstantiierte Behauptungen.' The reply named no specific finding, no file, and no technical basis for that characterization, while confirming that any supervisory-authority inquiry would receive a substantive answer. RFI-IRFOS asked the same day which of the four technical findings then on the table Tchibo considered factually incorrect; no answer followed before the embargo. Twice earlier in the case, 25 August and 15 September, Tchibo customer service had misread the disclosure as a business-partnership inquiry rather than a GDPR notice. A parallel Austrian-market thread, opened 28 July under REF AT-TCHIBO-2026-R1, received no reply of any kind at any point.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)	Hardcoded Firebase key in the production APK
C2	GDPR Art. 5(1)(c), Art. 6(1), Art. 13(1)(e), Art. 25	Auto-starting session replay capturing check-out/payment flows before consent
H1	GDPR Art. 13(1)(e), Art. 7(3), Art. 32(1)	Post-review tag deployment and a hardcoded attribution token
H2	GDPR Art. 5(1)(b), Art. 6(1)(a); TKG 2021 Sec. 165	Boot-time geofence registration independent of app use
H3	GDPR Art. 5(1)(c), Art. 6(1)(a), Art. 13(1)(c)	Redundant advertising-identifier mechanisms enabling cross-device profiling

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@tchibo.de , bcc Austrian DSB/CERT.at/Hamburg DPA; 2 CRITICAL + 3 HIGH findings
2026-07-28	Parallel Austrian-market thread opened to datenschutz@tchibo.at under REF AT-TCHIBO-2026-R1; never answered
2026-08-25	Tchibo customer service confirms a ticket, misreads the disclosure as forwarded to a 'Community' team
2026-09-15	Tchibo customer service misreads the disclosure as a business-cooperation offer; RFI-IRFOS clarifies the same day
2026-09-18	Datenschutz@tchibo.de sends its only substantive reply: a general denial naming no specific finding; RFI-IRFOS asks which of four findings is factually disputed; no answer follows
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Identify specifically which finding, if any, Tchibo disputes on the facts, with a technical basis, rather than a general characterization.
- Gate ContentSquare initialization behind an affirmative consent decision and exclude checkout/payment screens from capture.
- Rotate the exposed Firebase key and remove the hardcoded Adjust token.
- Register Emarsys geofences only after active, in-session app use, not automatically on every device boot.
- Consolidate to a single, disclosed advertising-identifier mechanism.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. GDPR Art. 5, 6, 7, 13, 25, 32. TKG 2021 Sec. 165. REF TCHIBO-2026-R1.