



Security & Privacy Disclosure, Final Report

Kaufland Android (com.kaufland.Kaufland)

Of five findings disclosed on 30 June 2026, one was independently retracted by RFI-IRFOS on 2 October 2026 after the current production build confirmed Kaufland's own counter-claim, one new finding was confirmed during that same re-verification, Kaufland disputed the remainder as factually and legally baseless and threatened defamation and criminal proceedings unless the public record was deleted, and declined further correspondence rather than answer three sharpened questions

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28 SEPTEMBER 2026, TWO SUBSTANTIVE REPLIES RECEIVED, ONE FINDING RETRACTED, ONE NEW FINDING CONFIRMED, REMAINDER DISPUTED, CORRESPONDENCE DECLARED CLOSED BY KAUFLAND

Target	Kaufland Stiftung & Co. KG, Neckarsulm (Schwarz Gruppe, Europe's largest grocery retailer by revenue)
Package	com.kaufland.Kaufland
Platform Audited	Android, static analysis of the production APK (re-verified 2026-10-02 against v6.18.0, versionCode 169892, sha256 d9a7692...df0cb5, pulled directly from a production device)
Initial Disclosure (R1)	2026-06-30, to security@kaufland.de and datenschutz@kaufland.de, CC presse@kaufland.de, Austrian Datenschutzbehoerde, CERT.at, EDPS and LfDI Baden-Wuerttemberg (BCC on R1, later moved to visible CC)
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	HIGH
Findings	5 originally disclosed: 1 retracted by RFI-IRFOS after independent re-verification confirmed Kaufland's counter-claim, 1 new finding confirmed during that same re-verification, 4 remain active (3 High, 1 Medium), 0 Critical after CVSS-consistent review
Correspondence	11 messages sent by RFI-IRFOS over 94 days (2026-06-30 to 2026-10-02), 2 substantive replies received (2026-09-22 and 2026-10-01, both from datenschutz@kaufland.de), disputing severity and legal characterization, threatening defamation and criminal referral unless the public record was deleted by 2026-10-06, and declaring the correspondence closed without answering RFI-IRFOS's final three questions
Authorities Notified	Austrian Datenschutzbehoerde (dsb@dsb.gv.at) · CERT.at · European Data Protection Supervisor (EDPS, edps@edps.europa.eu) · LfDI Baden-Wuerttemberg (lead authority for Kaufland's Neckarsulm headquarters)

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	Engagement Summary	5
4	Kaufland’s First Substantive Reply, 22 September 2026	6
5	Re-Verification Against the Current Production Build, 1-2 October 2026	7
6	Findings	8
6.1	C1: Two hardcoded Google API keys and a Firebase Realtime Database URL, permanently embedded and unrotatable once shipped	8
6.2	C2: LexisNexis ThreatMetrix device-fingerprinting code present, undisclosed in the privacy notice; Kaufland disputes active instantiation, not yet independently resolved	9
6.3	C3: Huawei HMS AAID provider initializes pre-consent (confirmed unchanged); re-verification additionally confirmed the Huawei OAID identifier is routed into the Adjust attribution SDK	10
6.4	H1: RETRACTED FOR CURRENT BUILD – Chucker HTTP Inspector	11
6.5	H2: Disney+ offer via Bluecode: Lidl Content GmbH is named as the contracting reseller, but neither Disney nor Disney+ is named anywhere in the specific privacy-notice clause Kaufland cites for it	11
7	Impact Analysis	12
8	The Complete Chain: Eleven Messages, 94 Days, One Retraction, One New Finding, Correspondence Declared Closed by Kaufland	12
9	Data Protection – Article by Article	13
10	Regulatory & Legal Landscape	13
11	Indicators of Compromise	14
12	Disclosure Timeline & Outcome	14
13	Residual Risk & Recommendations	15

Executive Summary

Kaufland's Android app (com.kaufland.Kaufland) is the mobile companion to Europe's largest grocery retail group by revenue, Schwarz Gruppe, offering self-scan checkout, Kaufland Pay, loyalty, and a digital-services marketplace that includes a Disney+ subscription offer routed through the Bluecode payment SDK. RFI-IRFOS's static analysis of the production APK on 30 June 2026 identified five findings: two hardcoded Google API keys and a Firebase Realtime Database URL; LexisNexis ThreatMetrix device-fingerprinting code capable of aggregating roughly 200 device parameters; Huawei Mobile Services location, advertising-ID, and push infrastructure; a full build of the Chucker HTTP debug-inspection library; and an undocumented data-sharing path to Disney+ via a Kaufland-authored Bluecode integration class.

Kaufland's Security/Data-Protection team (datenschutz@kaufland.de) replied substantively twice, on 22 September and 1 October 2026, after 84 days of no response beyond LfDI Baden-Wuerttemberg's automated receipt confirmations. Both replies disputed RFI-IRFOS's severity classifications and legal conclusions as factually and legally baseless, characterized RFI-IRFOS's optional paid-engagement tier as improperly linked to the free disclosure, and ultimately demanded the public record be deleted by 6 October 2026, threatening injunctive relief, damages for reputational harm, and criminal referral if it was not, while declaring that Kaufland would not respond to further inquiries.

RFI-IRFOS re-verified all four of Kaufland's specific counter-claims against a fresh copy of the then-current production build (v6.18.0, pulled from a device on 2 October 2026) before replying. One claim was confirmed outright: the current build contains only the no-op variant of the Chucker library, with zero internal implementation classes across all dex files, and RFI-IRFOS retracted that finding (originally H1) for the current build without qualification. The remaining three claims were each found to be partially accurate on a narrow reading while leaving the finding's actual, broader point unaddressed: the specific Firebase database instance is confirmed deactivated and returns HTTP 423, but the hardcoded key and database URL themselves remain permanently embedded and unrotatable in every distributed copy of the binary; the Huawei AAID provider's platform-mandated pre-consent initialization is unchanged, and re-verification additionally confirmed, as a new finding Kaufland's letter did not address at all, that the build separately reads the Huawei OAID identifier and routes it into the Adjust attribution SDK; and Lidl Content GmbH is genuinely named as the Disney+ offer's contracting party in the app and in a real clause of Kaufland's privacy notice, but that clause does not name Disney or Disney+ anywhere in its own text.

RFI-IRFOS communicated all of the above to Kaufland on 2 October 2026, together with three new, narrower questions, and declined to delete any finding that independent re-verification did not disprove. Kaufland has not replied since. The embargo of 28 September 2026 passed before Kaufland's final message was even sent. This report, published 19 days after the embargo, documents the retraction, the new finding, and the disputed remainder exactly as the correspondence itself establishes them, including Kaufland's demand for deletion and the legal consequences it threatened.

ID	Severity	Title
C1	HIGH	Two hardcoded Google API keys and a Firebase Realtime Database URL, permanently embedded and unrotatable once shipped

ID	Severity	Title
C2	HIGH	LexisNexis ThreatMetrix device-fingerprinting code present, undisclosed in the privacy notice; Kaufland disputes active instantiation, not yet independently resolved
C3	HIGH	Huawei HMS AAID provider initializes pre-consent (confirmed unchanged); re-verification additionally confirmed the Huawei OAID identifier is routed into the Adjust attribution SDK
H1	RETRACTED	RETRACTED FOR CURRENT BUILD – Chucker HTTP Inspector
H2	MEDIUM	Disney+ offer via Bluecode: Lidl Content GmbH is named as the contracting reseller, but neither Disney nor Disney+ is named anywhere in the specific privacy-notice clause Kaufland cites for it

Subject & Operator Context

Kaufland Stiftung & Co. KG, headquartered in Neckarsulm, Germany, is part of Schwarz Gruppe, Europe's largest grocery retail group by revenue, operating over 1,500 stores across 8 countries. The Kaufland Android app's self-scan, payment, and loyalty functions place it under the German BfDI/LfDI Baden-Wuerttemberg framework for Kaufland's own processing, while its use by Austrian customers gives the Austrian Datenschutzbehoerde an independent interest. All substantive correspondence in this case was conducted with datenschutz@kaufland.de, Kaufland's own data-protection mailbox, which signed its replies 'Team Datenrecht'.

Engagement Summary

RFI-IRFOS disclosed five findings on 30 June 2026 to security@kaufland.de and datenschutz@kaufland.de, with Kaufland's press office, the Austrian Datenschutzbehoerde, CERT.at, the EDPS, and LfDI Baden-Wuerttemberg in CC/BCC, stating an embargo of 28 September 2026. Seven follow-ups (6 July, 17 July, 24 July, 31 July, 9 August, 24 August, 31 August 2026) and an eighth on 12 September restated the three standing questions. Every one of these nine messages drew only LfDI Baden-Wuerttemberg's automated receipt confirmation; Kaufland itself did not reply for 84 days.

Kaufland's First Substantive Reply, 22 September 2026

On 22 September 2026, datenschutz@kaufland.de replied for the first time, disputing all five findings as based on static analysis that allegedly ignored the app's real runtime behaviour, data flows, and architecture, and asserting that RFI-IRFOS's conclusions were 'factually and legally incorrect.' The reply characterized RFI-IRFOS's optional paid-engagement tier, mentioned in the original R1 letter for findings beyond the five disclosed for free, as a commercial demand improperly linked to the disclosure, rejected it, and warned of legal consequences, including injunctive relief and damages for reputational harm, and potential criminal referral, if RFI-IRFOS's existing public statements were not deleted by 6 October 2026.

RFI-IRFOS replied the same day, clarifying first that the five findings at issue (C1-C3, H1, H2) were part of the free, public disclosure from the outset, structurally independent of the separately priced optional tier Kaufland's letter had cited, and second that Kaufland's runtime-behaviour objection did not rebut any claim RFI-IRFOS had actually made, since the original disclosure explicitly described these as static findings verifiable in the distributed binary without reproduction. RFI-IRFOS then addressed each of Kaufland's five rebuttal points individually: on C1, noted that Kaufland's reply addressed only the Maps key, not the more severe hardcoded Firebase database URL, and asked whether its security rules permit unauthenticated read access; on C2, stated it would independently verify Kaufland's claim that the LexisNexis ThreatMetrix classes are never instantiated at the next scheduled weekly diff, and would correct the finding publicly and explicitly if that claim held up; on C3, noted Kaufland's reply described the location service, which RFI-IRFOS had not disputed, while leaving the actual finding, the Huawei AAID provider's pre-consent initialization, unaddressed; on H1, noted Kaufland's no-op claim was independently checkable and would be verified at the next diff; and on H2, accepted the Disney/Lidl Content controller-reseller framing as a plausible answer to the processor-agreement question, while asking whether that reseller relationship is named as such in Kaufland's own privacy notice, not only during the Disney+ sign-up flow. RFI-IRFOS declined to delete any finding before the embargo and set three sharpened questions with a 6 October 2026 deadline of its own.

Re-Verification Against the Current Production Build, 1-2 October 2026

On 1 October 2026, datenschutz@kaufland.de replied a second and, by its own statement, final time: that the Firebase database's security rules deny unauthenticated access and that the instance is independently deactivated (HTTP 423); that the Huawei AAID provider and its resulting identifier serve the Huawei Push Kit exclusively, are never used for analytics, and are not linked to the Huawei advertising identifier (OAID); and that Lidl Content GmbH is named as the Disney+ offer's responsible reseller in clause 6.14 of Kaufland's privacy notice, with Disney's own specific disclosure obligation satisfied at the point a user actually opts into that optional service rather than at general app registration. The reply stated the matter was 'finally clarified' from Kaufland's side, that Kaufland would not respond to further inquiries, and repeated the demand to delete all existing public statements, this time without conceding that merely marking a finding closed while leaving its text in place would be sufficient.

Before replying, RFI-IRFOS independently re-verified each of these four claims against a fresh copy of the then-current production build, v6.18.0 (versionCode 169892, sha256 d9a7692800419b20602fe867d5801556704b66a92d1579c870e8466c5df0cb5), pulled directly from a production device on 2 October 2026. One claim, the Chucker no-op claim, was confirmed outright and the underlying finding (H1) was retracted for the current build without qualification. The other three were each found accurate on their own narrow terms while leaving the finding's broader point standing: the Firebase instance's HTTP 423 response was reproduced verbatim, but the hardcoded key and database URL remain permanently embedded in every distributed copy of the binary regardless of the backend's current state, and neither can be meaningfully rotated after the fact; the AAID provider's `initOrder` and the absence of any consent gate were confirmed unchanged, and re-verification additionally found, unaddressed anywhere in Kaufland's letter, that the build separately reads the Huawei OAID identifier and routes it into the Adjust attribution SDK via Kaufland's own code; and Lidl Content GmbH is genuinely named in clause 6.14, but that clause's own text never names Disney or Disney+, a fact the binary and the live privacy-notice page both independently confirm. RFI-IRFOS communicated all of this on 2 October 2026 with three new questions and declined to delete any finding re-verification had not disproven. Kaufland has not replied since; the correspondence record ends there as of this report's publication.

Findings

C1: Two hardcoded Google API keys and a Firebase Realtime Database URL, permanently embedded and unrotatable once shipped

HIGH, 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, 7.0 — Kaufland confirms the specific database instance now returns HTTP 423 (deactivated); this does not address the hardcoding itself

```
google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Kaufland in R1]
google_crash_reporting_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to
    Kaufland in R1]
google_map_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Kaufland in R1]
firebase_database_url: kaufland-app-android.firebaseio.com (confirmed HTTP 423 '
    deactivated' as of 2026-10-02, verified independently)
```

Impact: A Google API key (shared with Crash Reporting), a separate Google Maps key, and a Firebase Realtime Database URL are hardcoded in `res/values/strings.xml` of the production APK, confirmed present and unchanged in the 2026-10-02 re-verification build (v6.18.0). Kaufland's 1 October 2026 reply confirmed, and RFI-IRFOS independently reproduced verbatim on 2 October 2026, that a direct unauthenticated request to the database instance returns HTTP 423 with the message 'The Firebase database kaufland-app-android has been deactivated.' That response is consistent with either a fully deactivated project or locked-down security rules; both block the one test that is appropriate to run without authorization. It confirms only that this specific instance cannot be read right now, not that hardcoding an unrotatable key and database URL into a public binary was a safe practice: the values remain embedded, byte-identical, in every historical copy of the app already in circulation, and cannot be rotated without a full app-store update reaching every installed copy. Kaufland's reply addressed the Maps key specifically but did not dispute that the Firebase key and database URL are present and hardcoded.

C2: LexisNexis ThreatMetrix device-fingerprinting code present, undisclosed in the privacy notice; Kaufland disputes active instantiation, not yet independently resolved

HIGH, 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, 7.1 — DISPUTED: Kaufland states these classes are never instantiated at runtime; RFI-IRFOS has not independently confirmed or refuted this specific claim as of publication

```
com/lexisnexisrisk/threatmetrix/TMXProfilingHandle
com/lexisnexisrisk/threatmetrix/TMXConfigurationKeys
com/lexisnexisrisk/threatmetrix/TMXStrongAuth
com/lexisnexisrisk/threatmetrix/TMXProfilingConnectionsInterface
Status: presence confirmed by static analysis; active instantiation disputed by
      Kaufland, not independently verified
```

Impact: LexisNexis ThreatMetrix, a commercial device-intelligence SDK capable of aggregating roughly 200 device parameters (hardware fingerprint, sensors, network configuration, behavioural biometrics) into a Digital Identity profile, is confirmed present in the binary (TMXProfilingHandle, TMXConfigurationKeys, TMXStrongAuth, TMXProfilingConnectionsInterface classes). RFI-IRFOS's original finding was based on this static presence, consistent with its stated methodology of treating static, binary-verifiable findings as not requiring runtime reproduction. Kaufland's 22 September 2026 reply disputed this specifically, stating the classes are never instantiated, configured, or executed at runtime and that no processing under Art. 4(2) GDPR therefore occurs. RFI-IRFOS stated on the same day that it would verify the instantiation path at the next scheduled weekly binary diff and correct the finding publicly if Kaufland's claim held up; no such verification is reflected in the correspondence as of this report's publication, and this finding is presented here with Kaufland's dispute stated plainly rather than resolved either way. No Art. 44-49 transfer mechanism or explicit purpose for ThreatMetrix was identified in Kaufland's available privacy information independent of this dispute.

C3: Huawei HMS AAID provider initializes pre-consent (confirmed unchanged); re-verification additionally confirmed the Huawei OAID identifier is routed into the Adjust attribution SDK

HIGH, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 7.2 — platform-mandated pre-consent init confirmed unchanged on 2026-10-02; OAID-to-Adjust wiring is a new finding confirmed the same day, not addressed in Kaufland's letter

```
<provider android:name="com.huawei.hms.aaid.InitProvider" android:initOrder="500"
  android:exported="false"/>
com.huawei.hms.ads.identifier.AdvertisingIdClient -- Huawei OAID, distinct from AAID
com/adjust/sdk/oaid/AdjustOaid, HmsSdkClient, MsaSdkClient -- Adjust SDK's OAID read
  path
kaufland/com/analytics/adjust/OaidLogger -- Kaufland-authored wrapper routing OAID
  into Adjust
No tools:node="remove" suppression of the AAID provider present in the manifest
```

Impact: com.huawei.hms.aaid.InitProvider is declared with initOrder=500 and is auto-instantiated by the Android OS before any Activity, and therefore before any consent dialog, can load; this is unchanged and confirmed in the 2026-10-02 re-verification build. Kaufland's 1 October 2026 reply correctly describes this ContentProvider auto-init as standard Android platform behaviour and states the resulting AAID serves Huawei Push Kit routing exclusively, is never used for analytics, and is not linked to the Huawei advertising identifier (OAID). Re-verification confirmed the AAID/push-routing/no-analytics-product claims are plausible on static evidence and could not be fully disproven without a full call-graph trace, but it also found, unaddressed anywhere in Kaufland's two replies, that the current build separately reads the Huawei OAID identifier (com.huawei.hms.ads.identifier.AdvertisingIdClient, distinct from AAID, as Kaufland's own letter correctly distinguishes) and routes it into the Adjust attribution SDK via com/adjust/sdk/oaid/AdjustOaid and a Kaufland-authored wrapper, kaufland/com/analytics/adjust/OaidLogger. Kaufland's own location-service response states this Huawei code path activates only on devices without functional Google services, under 1% of its user base by its own account; RFI-IRFOS has not independently confirmed that same population bound applies to the OAID/Adjust path specifically, and presents it here as a newly confirmed, un-rebutted finding rather than an extension of Kaufland's own figure.

H1: RETRACTED FOR CURRENT BUILD – Chucker HTTP Inspector

RETRACTED 2026-10-02 – current production build ships only the Chucker no-op library variant, confirmed by independent re-verification

Impact: RFI-IRFOS's original 30 June 2026 finding stated that the full Chucker HTTP-inspection library, capable of logging request headers, response bodies, and authentication tokens to a local database, shipped in the production APK. Kaufland's 22 September 2026 reply stated that only the library-no-op artifact, consisting entirely of empty stub classes with no interception or storage logic, is compiled into production builds. RFI-IRFOS re-verified this independently on 2 October 2026 against the then-current production build (v6.18.0): zero `com.chuckerteam.chucker.internal.*` classes exist anywhere across all 20 dex files, only the public API surface, which is the specific, confirming signature of a no-op-only build. RFI-IRFOS retracted this finding for the current build without qualification on 2 October 2026, consistent with its standing practice of correcting any finding that independent re-verification disproves. This finding is retained here, marked retracted, rather than deleted, as the honest record of what was originally found, disputed, and subsequently confirmed wrong for the current build; no assertion is made about builds prior to 2026-10-02, since no APK or hash from the original June analysis was retained for direct comparison.

H2: Disney+ offer via Bluecode: Lidl Content GmbH is named as the contracting reseller, but neither Disney nor Disney+ is named anywhere in the specific privacy-notice clause Kaufland cites for it

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 4.6 — downgraded from the original HIGH finding after re-verification narrowed it to a transparency-precision gap rather than an undisclosed data-sharing relationship

```
In-app: disney_plus_invoice_company_name = "Lidl Content GmbH"
Live clause 6.14 (Kaufland Card XTRA Datenschutzhinweise): names "Lidl Content GmbH"
    as contracting party;
    does not contain the word "Disney" anywhere in its own text
Payment data: not listed among fields transmitted to Lidl Content GmbH per clause 6.14
```

Impact: RFI-IRFOS's original finding identified a Kaufland-authored Bluecode class, `BlueCodeDisneyPlusManagerImpl`, linking Kaufland payment and purchase behaviour to Disney+ subscription status, and did not find this disclosed as a data-sharing relationship. Kaufland's replies state that Disney acts as an independent controller for the Disney+ service itself, that Lidl Content GmbH acts as the responsible reseller handling the contractual relationship under Art. 6(1)(b)/(f), and that this is disclosed in clause 6.14 of Kaufland's Kaufland Card XTRA privacy notice plus a separate notice shown during Disney+ sign-up. RFI-IRFOS independently confirmed, by reading the live clause 6.14 directly on 2026-10-02, that Lidl Content GmbH is indeed named there as the contracting party for 'digital services,' including identification numbers, subscription dates, name, email, phone, and address fields transmitted to it, with payment data notably absent from that list, consistent with Kaufland's claim that payment data is not shared with Disney. However, clause 6.14 itself is a generic digital-services clause: the word 'Disney' does not appear in it anywhere, and in-app strings naming Dis-

ney+ specifically exist only in separate FAQ/summary screens, not in the clause Kaufland's own letter cites as satisfying Art. 13 for this relationship. Whether a generic clause plus a just-in-time, service-specific notice together satisfy Art. 13 for this particular service is a legal question a binary and a privacy-notice page cannot resolve on their own; what both independently confirm is which company is named where.

Impact Analysis

This case differs from a silent one: Kaufland engaged twice, in detail, and RFI-IRFOS's own re-verification against a fresh production build confirmed that one of the five original findings (H1, Chucker) was genuinely wrong for the current build and retracted it the same day re-verification completed. That same re-verification pass also surfaced a new, confirmed finding (the Huawei OAID-to-Adjust wiring in C3) that neither side had previously raised. The three remaining findings (C1, C2, C3's AAID component, and H2) were each addressed by Kaufland on a narrower reading than the finding actually made, leaving the broader point in each case un-rebutted rather than resolved. Kaufland's characterization of the entire disclosure as demonstrably false, and its demand that the public record be deleted under threat of defamation and criminal proceedings, is itself part of the record this report documents; RFI-IRFOS's response throughout was to retract what independent re-verification disproved and maintain, with evidence, what it did not.

The Complete Chain: Eleven Messages, 94 Days, One Retraction, One New Finding, Correspondence Declared Closed by Kaufland

Step 1 – Disclosure sent: RFI-IRFOS discloses five findings on 30 June 2026 to security@kaufland.de and datenschutz@kaufland.de, CC/BCC Kaufland's press office, the Austrian Datenschutzbehörde, CERT.at, the EDPS, and LfDI Baden-Wuerttemberg, stating an embargo of 28 September 2026.

Step 2 – Extended silence: Nine messages (the original disclosure plus eight follow-ups: 6 July, 17 July, 24 July, 31 July, 9 August, 24 August, 31 August, 12 September 2026) draw nothing from Kaufland itself, only LfDI Baden-Wuerttemberg's automated receipt confirmations, across 84 days.

Step 3 – First substantive reply: On 22 September 2026, datenschutz@kaufland.de disputes all five findings, objects to RFI-IRFOS's optional paid tier as improperly linked to the disclosure, and sets a 6 October 2026 deletion deadline with legal threats attached. RFI-IRFOS replies the same day, clarifies the five findings were always part of the free disclosure, addresses each rebuttal point individually, and sets three sharpened questions of its own.

Step 4 – Second and final reply: On 1 October 2026, datenschutz@kaufland.de answers the three sharpened questions, declares the matter finally clarified from Kaufland's side, states it will not respond further, and repeats the deletion demand in stronger terms.

Step 5 – Independent re-verification: On 2 October 2026, RFI-IRFOS pulls a fresh copy of the then-current production build (v6.18.0) directly from a device and tests each of Kaufland's four specific counter-claims against it before replying.

Step 6 – One retraction, one new finding: RFI-IRFOS retracts H1 (Chucker) outright, confirms C1's narrow database-deactivation claim while maintaining the broader hardcoding point, confirms C3's AAID/no-analytics-product claims while surfacing the new, unaddressed OAID-to-Adjust finding, and confirms H2's Lidl Content naming while noting Disney itself

is unnamed in the cited clause. RFI-IRFOS declines to delete any finding re-verification did not disprove and sends three new questions.

Step 7 – Silence resumes: Kaufland does not reply after 2 October 2026, consistent with its own stated intention to end the correspondence. The embargo of 28 September 2026 had already passed before Kaufland's final message was even sent.

Step 8 – Publication: This report publishes 19 days after the embargo, documenting the retraction, the new finding, and the disputed remainder exactly as the correspondence establishes them.

Data Protection – Article by Article

Art. 32(1)(b) GDPR – Security of processing: C1's hardcoded, unrotatable API keys and database URL fall short of this provision regardless of whether the specific backend instance is reachable today.

Art. 13, Art. 6(1), Art. 44-49 GDPR – Transparency, lawfulness, third-country transfer: C2's LexisNexis ThreatMetrix code is present and undisclosed in available privacy information; whether it is actively instantiated remains disputed and unresolved as of publication.

Art. 44-49, Art. 13, Art. 7 GDPR – Third-country transfer, transparency, conditions for consent: C3's Huawei AAID pre-consent initialization is platform-mandated and confirmed unchanged; the newly confirmed OAID-to-Adjust routing raises the same transparency and lawful-basis questions independently of the AAID point.

Art. 13 GDPR – Information to be provided: H2's clause 6.14 names the correct contracting party (Lidl Content GmbH) but not the underlying service (Disney+) it covers, a precision gap rather than an absent disclosure.

Regulatory & Legal Landscape

Kaufland Stiftung & Co. KG's Neckarsulm headquarters places LfDI Baden-Wuerttemberg as the lead supervisory authority for Kaufland's own processing; the Austrian Datenschutzbehörde, CERT.at, and the EDPS were copied throughout per RFI-IRFOS's standing practice. Kaufland's correspondence twice characterized RFI-IRFOS's findings as demonstrably false statements causing reputational harm and threatened injunctive relief, damages, and criminal referral unless the public record was deleted by 6 October 2026. RFI-IRFOS's position throughout this correspondence, and in this report, has been to retract any specific claim that independent, evidence-based re-verification against the actual production binary disproves (as it did with H1), and to maintain, with the same evidentiary standard, any claim it does not. No finding in this report asserts more than what static analysis of the binary and, where applicable, the live privacy-notice text actually show; disputed points not independently resolved (C2's instantiation question) are presented as disputed, not as settled fact.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 32 issue in C1, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 13, Art. 6, and Art. 44-49 issues in C2, C3, and H2, up to EUR 20,000,000 or 4% of total worldwide annual turnover.

Indicators of Compromise

The following findings were extracted from static analysis of the production APK, re-verified on 2026-10-02 against v6.18.0 (versionCode 169892, sha256 d9a7692800419b20602fe867d5801556704b66a92d1579c870e8466c5df0cb5), pulled directly from a production device. No Kaufland servers, accounts, or infrastructure were probed beyond one unauthenticated HTTP GET to confirm the Firebase database's public deactivation status. The hardcoded keys referenced in C1 are withheld from this public report; full values were disclosed privately to Kaufland in the original R1 letter.

```
C1 -- Hardcoded Google/Firebase keys + database URL, redacted in this public report;
      database instance independently confirmed deactivated (HTTP 423), hardcoding point
      stands

C2 -- LexisNexis ThreatMetrix classes present; active instantiation disputed by
      Kaufland,
      not independently resolved

C3 -- Huawei AAID initOrder=500 pre-consent, confirmed unchanged;
      NEW: Huawei OAID routed into Adjust SDK, confirmed 2026-10-02, not addressed by
      Kaufland

H1 -- RETRACTED: Chucker no-op-only confirmed, zero internal.* classes present

H2 -- Lidl Content GmbH named as Disney+ reseller in-app and in live clause 6.14;
      clause 6.14 itself does not name Disney or Disney+
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure (five findings) sent to security@kaufland.de and datenschutz@kaufland.de, CC/BCC press office, Austrian Datenschutzbehörde, CERT.at, EDPS, LfDI Baden-Wuerttemberg. Embargo stated as 2026-09-28.

2026-07-06 through 2026-09-12 Eight follow-ups sent. Each draws only LfDI Baden-Wuerttemberg's automated receipt confirmation; no reply from Kaufland.

2026-09-22 datenschutz@kaufland.de replies for the first time: disputes all five findings, objects to the paid-tier characterization, sets a 2026-10-06 deletion deadline with legal threats attached.

2026-09-22 RFI-IRFOS replies same day: clarifies the five findings were always part of the free disclosure, addresses each rebuttal point, sets three sharpened questions with a 2026-10-06 deadline of its own.

2026-09-28 Embargo date reached and passed.

2026-10-01 datenschutz@kaufland.de replies a second time: answers the three sharpened questions, declares the matter closed from Kaufland's side, states it will not respond further, repeats the deletion demand.

2026-10-02 RFI-IRFOS pulls and re-verifies the then-current production build independently, retracts H1 (Chucker), confirms the new OAID-to-Adjust finding within C3, narrows C1 and H2, and replies with three new questions. No reply from Kaufland since.

2026-10-17 This report published, 19 days after the embargo. Correspondence record: eleven RFI-IRFOS messages, two substantive Kaufland replies, one retraction, one new confirmed finding, three findings maintained in narrowed or disputed form, correspondence declared closed by Kaufland without its final three questions answered.

Residual Risk & Recommendations

C1 – Rotate the Firebase and Maps API keys in the next release regardless of the current database's deactivation status, and restrict both to the production signing certificate going forward so future keys are not permanently exposed by a single binary release.

C2 – Kaufland should publish, or provide RFI-IRFOS or a supervisory authority, verifiable evidence (such as an instrumented build or a signed statement to the LfDI) that the LexisNexis ThreatMetrix classes are genuinely never instantiated, resolving the one point this report leaves open as disputed rather than settled.

C3 – Address the newly confirmed Huawei OAID-to-Adjust routing with the same specificity Kaufland applied to the AAID/push-only claim: state plainly whether OAID data reaches Adjust for attribution or analytics purposes, on what legal basis, and where this is disclosed.

H2 – Name Disney or Disney+ explicitly within clause 6.14 itself, rather than relying on a generic digital-services clause plus a separate in-app notice to jointly satisfy Art. 13 for this specific service.

Procedural: RFI-IRFOS retracted the one finding (H1) that independent re-verification against the actual production binary disproved, the same day that verification completed, without requiring a legal threat to do so. The three findings that remain in this report survived that same evidentiary standard; RFI-IRFOS remains open to a further substantive reply, including the evidence requested on C2 and C3, at any time, and will update this report's public record if one arrives.

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, re-verified on 2026-10-02 against production build v6.18.0 (sha256 d9a7692800419b20602fe867d5801556704b66a92d1579c870e8466c5df0cb5), plus one unauthenticated HTTP GET to confirm a publicly stated database deactivation status. No other Kaufland servers, accounts, or infrastructure were probed. The hardcoded credentials referenced in finding C1 are withheld from this public report; full values were disclosed privately to Kaufland in the original R1 letter and remain available to Kaufland or to a supervisory authority on request. One finding (H1) was independently retracted for the current build after re-verification confirmed Kaufland's counter-claim; this is documented above rather than removed, as the honest record of what was found, disputed, and corrected. 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 COM.KAUFLAND.KAUFLAND.