



Security & Privacy Disclosure, Final Report

kicker Android (com.netbiscuits.kicker)

A Russian ad SDK adapter and a global cleartext opt-in inside a heavy ad-tech football app, eight messages over 73 days drew one automated ticket acknowledgment and no human reply, and none of the three questions on record was ever answered

PUBLIC DISCLOSURE, 17 OCTOBER 2026 - EMBARGO REACHED 29 SEPTEMBER 2026, EIGHT MESSAGES SENT, ONE AUTOMATED ACKNOWLEDGMENT, NO HUMAN REPLY, THREE QUESTIONS NEVER ANSWERED

Target	Olympia-Verlag GmbH, Nuremberg, Germany. Operator inferred from the binary; privacy contacts datenschutz@kicker.de and info@kicker.de
Package	com.netbiscuits.kicker v7.12.2 (versionCode 926)
Platform Audited	Android, static analysis of the production APK
Initial Disclosure (R1)	2026-07-01, to datenschutz@kicker.de and info@kicker.de, BCC BayLDA, Austrian Datenschutzbehoerde and EDPS
Disclosure / Embargo Date	2026-09-29
Report Published	2026-10-17
Overall Severity	HIGH
Findings	5 (2 High, 3 Medium, 0 Critical)
Correspondence	8 messages sent by RFI-IRFOS over 73 days (2026-07-01 to 2026-09-12). 1 automated Zendesk acknowledgment (ticket 347026, 2026-07-01), 0 human replies, 0 bounces, 0 of 3 questions answered
Authorities Notified	Bayerisches Landesamt fuer Datenschutzaufsicht (poststelle@lda.bayern.de, BCC) · Austrian Datenschutzbehoerde (dsb@dsb.gv.at) · European Data Protection Supervisor (EDPS, edps@edps.europa.eu)
SHA-256 (base APK)	a68a137cf1603d3a1b9e8f80ea86db367000a18ffd400c0508c6489822c9b94b

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	Findings	5
4.1	H1: Russian ad SDK adapter (Yandex Mobile Ads) bundled in a German publisher's app	5
4.2	H2: Network Security Config permits cleartext traffic for all domains	6
4.3	M1: Extensive advertising and attribution stack with broad pre-consent auto-initialisation	6
4.4	M2: Extractable Google/Firebase and geo API keys	7
4.5	M3: Piano ID and paywall behavioural profiling backend	7
5	Impact Analysis	8
6	The Complete Chain: Eight Messages, 73 Days, One Automated Ticket, Zero Human Replies	8
7	Data Protection – Article by Article	8
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	9
10	Disclosure Timeline & Outcome	9
11	Residual Risk & Recommendations	10

Executive Summary

kicker is a heavy ad-tech monetisation client wrapped around a football news app. Static analysis of production APK v7.12.2 (base.apk sha-256 a68a137c...9b94b) found two HIGH and three MEDIUM findings and no CRITICAL finding. The first HIGH finding is a bundled Yandex Mobile Ads adapter, a Russian ad SDK namespace, in a mainstream German publisher's app. The second is a Network Security Config that permits cleartext traffic for all domains on targetSdk 36.

The binary also carries more than fifteen advertising, attribution and profiling SDKs, several of which start at process start, two extractable Google API keys, and a Piano ID and payroll profiling backend.

kicker also has a strong consent posture on paper, and the original disclosure said so first: a full Usercentrics TCF CMP, Google consent-mode defaults set to deny in the manifest, Facebook auto-init and advertiser-ID collection disabled, allowBackup set to false, an AppHarbor ad-quality layer and no Chinese SDK.

RFI-IRFOS sent the disclosure on 1 July 2026 and seven follow-ups through 12 September 2026. The only response was an automated Zendesk acknowledgment generated within seconds of the first message. No human replied in 73 days, and the embargo of 29 September 2026 passed unanswered. This report publishes 18 days after the embargo with the full record intact.

ID	Severity	Title
H1	HIGH	Russian ad SDK adapter (Yandex Mobile Ads) bundled in a German publisher's app
H2	HIGH	Network Security Config permits cleartext traffic for all domains
M1	MEDIUM	Extensive advertising and attribution stack with broad pre-consent auto-initialisation
M2	MEDIUM	Extractable Google/Firebase and geo API keys
M3	MEDIUM	Piano ID and payroll behavioural profiling backend

Subject & Operator Context

RFI-IRFOS identified Olympia-Verlag GmbH, Nuremberg, as the operator of com.netbiscuits.kicker, inferred from the Olympia-Verlag string in the binary. The app is built by Tickaroo (com.tickaroo.*). The binary exposes no privacy contact, so the disclosure went to datenschutz@kicker.de and info@kicker.de. Olympia-Verlag is domiciled in Bavaria, so the Bayerisches Landesamt fuer Datenschutzaufsicht in Ansbach is the inferred lead supervisory authority, and it was in BCC from the first message.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 1 July 2026 to datenschutz@kicker.de and info@kicker.de, with the BayLDA, the Austrian Datenschutzbehoerde and the EDPS in BCC, stating an embargo date of 29 September 2026. The letter led with the app's consent strengths, then presented the two HIGH findings and the medium notes, and asked three questions: why a German news app contains a Russian ad SDK adapter, whether it is active and whether a transfer impact assessment under Art. 44-49 exists; on what basis the Network Security Config permits cleartext for all domains on targetSdk 36; and whether a data protection impact assessment under Art. 35 and joint-controller agreements under Art. 26 exist for the stack of more than fifteen advertising and attribution SDKs.

Seven follow-ups were sent (6 July, 17 July, 27 July, 15 August, 24 August, 31 August and 12 September 2026). From 15 August the Austrian Datenschutzbehoerde and the EDPS appeared in visible CC. The only response in the entire thread is the automated Zendesk acknowledgment of 1 July 2026 (ticket 347026), generated seconds after the first message. No human replied and no message bounced.

Findings

H1: Russian ad SDK adapter (Yandex Mobile Ads) bundled in a German publisher's app

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, 5.3 - adapter classes shipped, operator to document use and transfer basis

```
dex/classes*.dex:
  Lcom/yandex/mobile/ads/common/
  Lcom/yandex/mobile/ads/banner/
  Lcom/yandex/mobile/ads/interstitial/
  Lcom/yandex/mobile/ads/rewarded/
AppMetrica classes: none   Yandex endpoint strings: none
```

Impact: The dex files contain the com.yandex.mobile.ads namespace (common, banner, interstitial, rewarded). The footprint is about 14 classes, with no Yandex endpoint string and no AppMetrica classes, which fits a mediation adapter rather than the full SDK. Static analysis establishes that the adapter ships in the production binary. Whether it is switched on in production and where it sends bid and impression data is a question the operator can

answer from its mediation configuration, and it is the first of the three questions on record. Ad delivery through a vendor associated with a Russian-headquartered group routes device and ad-ID signals toward infrastructure outside the EU, which calls for disclosure and a transfer impact assessment. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.3 to HIGH because a mass-market German publisher ships a third-country ad supply chain, a supply-chain exposure that the CVSS technical scope does not capture.

H2: Network Security Config permits cleartext traffic for all domains

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, 5.3 - global cleartext opt-in across an SDK-heavy app

```
<base-config cleartextTrafficPermitted="true">
  (no domain-config restricting the scope)
targetSdk: 36 (platform default: cleartext denied)
```

Impact: res/xml/network_security_config.xml sets base-config cleartextTrafficPermitted="true" with no per-domain restriction. On targetSdk 36 the platform default is deny, so this is an explicit opt-in. Any HTTP endpoint used by the app or by its many advertising SDKs is exposed to interception and injection on a hostile network. The debug-overrides block that trusts user CAs applies to debuggable builds only and is not a production concern. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.3 to HIGH because the permission applies to the network traffic of 15 or more advertising and attribution SDKs in a mass-market German sport app.

M1: Extensive advertising and attribution stack with broad pre-consent auto-initialisation

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 - SDK breadth and process-start providers

```
line 168 com.taboola.android.TBLContextProvider (initOrder=0)
line 242 de.agmammc.agmasdk.android.AgmaContentProvider (initOrder=101)
line 245 com.google.android.gms.ads.MobileAdsInitProvider (initOrder=100)
line 221 de.infonline.lib.iomb.core.IOLInitProvider
line 307 com.facebook.ads.AudienceNetworkContentProvider
line 305 com.google.firebase.provider.FirebaseInitProvider (initOrder=100)
```

Impact: The class inventory shows InMobi, Usercentrics, Prebid Mobile, Taboola, INFOnline IOMB, AppHarbr, AppsFlyer, Piano, AppNexus/Xandr, AGMA, PubMatic, Amazon APS, Adjust, Facebook Audience Network and Google Ad Manager. Several components start through ContentProviders at process start: Taboola (initOrder 0), AGMA (initOrder 101), Google MobileAds (initOrder 100), INFOnline, Facebook Audience Network and Firebase (initOrder 100). Even with the Usercentrics CMP present, ContentProvider-based auto-init can execute measurement and attribution logic before a consent decision, and the number of downstream controllers raises Art. 26 and Art. 13 transparency duties.

M2: Extractable Google/Firebase and geo API keys

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 - key restriction status is for the operator to document

```
res/values/strings.xml -> Firebase API key: [REDACTED IN PUBLIC REPORT -- disclosed  
privately to kicker in R1]  
AndroidManifest.xml line 208 -> geo/Maps API key: [REDACTED IN PUBLIC REPORT --  
disclosed privately to kicker in R1]
```

Impact: Two Google API keys are embedded in the app, one Firebase key in the string resources and one geo/Maps key in the manifest, together with the Firebase project identifiers. Such keys are not secret by design, but unrestricted keys enable quota and billing exhaustion. Showing that package-name and SHA-1 restrictions and a per-API allow-list are in place rests with the operator. The key values are withheld from this public report.

M3: Piano ID and paywall behavioural profiling backend

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 4.8 - profiling backend needs documented basis

```
https://c2.piano.io  
https://buy-eu.piano.io  
io/piano/* (378 classes)
```

Impact: io.piano.android.* (378 classes) with endpoints buy.piano.io and c2.piano.io, plus regional EU, AP and AU variants and a sandbox endpoint. Piano Composer and ID is a subscription and behavioural-analytics platform, so reading behaviour is tied to a persistent Piano user profile. Disclosure and legal-basis obligations apply.

Impact Analysis

The findings are fixable engineering and documentation gaps, not evidence of malicious design, and the consent posture on paper is genuinely strong. What sets this case apart is the correspondence: eight messages over 73 days to two privacy-relevant mailboxes, a ticketing system that opened a ticket and never produced a human response, and a Russian ad SDK question that nobody at the company engaged with.

The Complete Chain: Eight Messages, 73 Days, One Automated Ticket, Zero Human Replies

Step 1 – Disclosure sent: RFI-IRFOS sends the full findings on 1 July 2026 to datenschutz@kicker.de and info@kicker.de, with the BayLDA, the Austrian Datenschutzbehörde and the EDPS in BCC, stating an embargo of 29 September 2026.

Step 2 – Automated acknowledgment only: seconds later the Zendesk system at datenschutz@kicker.zendesk.com confirms receipt as ticket 347026. This is the only response in the thread and no human follows it.

Step 3 – Silence: follow-ups on 6 July, 17 July and 27 July 2026 restate the findings and the three questions. No reply.

Step 4 – Silence continues, regulators in visible CC: follow-ups on 15 August, 24 August, 31 August and 12 September 2026. No human reply.

Step 5 – Embargo passes unanswered: 29 September 2026 passes with no human response and no delivery failure on record.

Step 6 – Publication: this report publishes 18 days after the embargo, with eight messages sent, one automated acknowledgment, zero human replies and zero of three questions answered.

Data Protection – Article by Article

Art. 44-49 GDPR – Third-country transfers: H1's Yandex adapter requires a documented transfer mechanism and impact assessment if it is active.

Art. 32 and Art. 5(1)(f) GDPR – Security of processing: H2's global cleartext opt-in and M2's unrestricted-key exposure.

Art. 6, Art. 7 and Art. 5(1)(c) GDPR – Lawfulness, consent and minimisation: M1's SDK breadth and process-start providers.

Art. 26 GDPR – Joint controllership: the number of downstream advertising controllers requires documented arrangements.

Art. 13 and Art. 14 GDPR – Transparency: M3's Piano profile and the full list of recipients must be named in the privacy information.

Regulatory & Legal Landscape

The Bayerisches Landesamt fuer Datenschutzaufsicht is the inferred lead supervisory authority for Olympia-Verlag GmbH and was in BCC from the original disclosure. The Austrian Datenschutzbehoerde and the EDPS were in BCC from the original disclosure and in visible CC from 15 August 2026.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 26 and Art. 32 issues in H2, M1 and M2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 44-49, Art. 6, Art. 7, Art. 13 and Art. 14 issues in H1, M1 and M3, up to EUR 20,000,000 or 4% of total worldwide annual turnover.

Indicators of Compromise

The following items were extracted from the published production APK via static analysis only. No kicker servers, accounts, or infrastructure were probed. The two Google API keys referenced in M2 are withheld from this public report; full values were disclosed privately to kicker in the original R1 letter.

```
H1 -- com/yandex/mobile/ads/{common,banner,interstitial,rewarded} in dex
H2 -- res/xml/network_security_config.xml: base-config cleartextTrafficPermitted=true
M1 -- Taboola, AGMA, MobileAds, INFOnline, Facebook AN, Firebase providers
M2 -- Firebase and geo API keys (redacted)
M3 -- io.piano.android.*, buy.piano.io, c2.piano.io
```

Disclosure Timeline & Outcome

2026-07-01 Initial disclosure sent to datenschutz@kicker.de and info@kicker.de, BCC BayLDA, Austrian Datenschutzbehoerde and EDPS. Embargo stated as 2026-09-29.

2026-07-01 Automated Zendesk acknowledgment received (ticket 347026). No human content.

2026-07-06 Follow-up sent. No reply.

2026-07-17 Follow-up sent. No reply.

2026-07-27 Follow-up sent. No reply.

2026-08-15 Follow-up sent, Austrian Datenschutzbehoerde and EDPS in visible CC. No reply.

2026-08-24 Follow-up sent. No reply.

2026-08-31 Follow-up sent, both regulators in visible CC. No reply.

2026-09-12 Follow-up sent, 73 days since the original disclosure. No reply.

2026-09-29 Embargo date reached and passed with all three questions unanswered.

2026-10-17 This report published, 18 days after the embargo date. Correspondence record: eight RFI-IRFOS messages, one automated acknowledgment, zero human replies, zero bounces, zero of three questions answered.

Residual Risk & Recommendations

H1 – State whether the Yandex adapter is active in production, remove it if it is not needed, and document a transfer impact assessment if it is.

H2 – Replace the global cleartext permission with HTTPS everywhere, or scope cleartext to named legacy domains in a domain-config.

M1 – Defer ContentProvider-based SDK initialisation until the Usercentrics decision is recorded, and document Art. 26 arrangements for the ad stack.

M2 – Restrict both Google API keys to the production signing certificate and the APIs actually used, then rotate them.

M3 – Name Piano as recipient and processor in the privacy information and document the legal basis for the profile.

Procedural: RFI-IRFOS remains open to a substantive human reply to the three questions at any time; this report will be updated to reflect one if it 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 pub-

lished application using publicly available tooling. No kicker servers, accounts, or infrastructure were probed. Credential values are withheld from this public report and were disclosed privately to kicker in the original R1 letter. Analysis by RFI-IRFOS, ZVR 1015608684, GISA 39261441, Steuernummer 68 696/8736. REF KICKER-2026-R1-001.