



Security & Privacy Disclosure, Final Report

Binance (com.binance.dev) v3.16.7

A China-headquartered behavioral-analytics SDK that initializes before any consent screen, four exported and unguarded JPush/Jiguang components, and a self-disclosed China remote-access nexus in Binance's own privacy notice, met by seven automated or templated responses over 60 days, one redirect to a bug-bounty program, and no answer to any of three questions

PUBLIC DISCLOSURE, 17 OCTOBER 2026. EMBARGO REACHED 30 SEPTEMBER 2026, TWO HIGH FINDINGS UNADDRESSED ON THE MERITS

Target	Nest Exchange Limited, Nest Trading Limited and Nest Clearing and Custody Limited (Abu Dhabi Global Market), operating the Binance platform; EU Article 27 representative VeraSafe Ireland Ltd (Cork)
Package	com.binance.dev (versionCode 100301607)
Platform	Android, static analysis (base.apk 240.9 MB, 22 classes*.dex files, roughly 200 MB of compiled code, the largest app in this audit series)
Initial Disclosure (R1)	2026-07-02 (REF BINANCE-2026-R1-001)
Disclosure / Embargo Date	2026-09-30
Report Published	2026-10-17
Overall Severity	HIGH
Findings	4 plus 1 architecture observation (2 High, 1 Medium, 1 Low; MiCA verdict PARTIAL)
Correspondence	7 messages sent by RFI-IRFOS over 60 days (2 July through 31 August 2026) to dpo@binance.com and pr@binance.com, with the Austrian DSB and the EDPS in copy. Two of the seven (6 July and 7 July) were rejected by Gmail for all four recipients (status 5.7.1) and never reached Binance; the 27 July resend and the 9 August, 24 August and 31 August follow-ups were accepted. Binance responded with seven automated or templated messages: a PR-team auto-reply (2 July), five identical Data Protection Office acknowledgments (2 July, 27 July, 9 August, 24 August and 31 August), and one different templated message on 7 July stating the enquiry falls outside the DPO team's scope and pointing to the Binance Bug Bounty Program on Bugcrowd while also inviting a data-protection submission. RFI-IRFOS confirmed in writing that this is a data-protection matter; no further response followed. None of the three questions was answered.
Authorities CC'd	Österreichische Datenschutzbehörde (DSB), Austria; European Data Protection Supervisor (EDPS)
SHA-256 (base APK)	ae09cdf34608cec818e6d6e37b82e5fdc828060056cd0b223ab49a5899e40318

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	6
4.1	H1: SensorsData (China) behavioral-analytics ContentProvider initializes before any consent screen can render	6
4.2	H2: JPush/Jiguang: two exported services and two exported content providers without any permission guard	7
4.3	M1: Chinese-vendor SDK inventory: JPush/Jiguang and SensorsData confirmed; Nezha and Agora resolved and dropped	8
4.4	L1: No TLS certificate pinning; cleartext correctly blocked app-wide; no user-CA trust in the release path	8
5	Impact Analysis	9
6	The Complete Chain: Seven Messages Sent, Seven Automated Responses, Zero Answers	9
7	Disclosure Timeline & Outcome	10
8	MiCA / EU Jurisdiction-Gating Thesis: Test Result PARTIAL	10
9	Informational: Credential Hygiene Result	11
10	What Binance Got Right	11
11	Data Protection Article by Article	12
12	Regulatory Landscape & Fine Exposure	12
13	Indicators of Compromise	13
14	Residual Risk & Recommendations	13

Executive Summary

Binance's Android application (com.binance.dev v3.16.7) is the largest app RFI-IRFOS has analyzed in this series: 22 dex files and roughly 200 MB of compiled code. A static analysis cross-checked with an independent aapt2 manifest dump and Binance's own privacy notice of 5 January 2026 identified two HIGH findings, one MEDIUM and one LOW, plus an architecture observation on EU MiCA gating. No CRITICAL finding is issued.

The strongest result is a China data-access chain corroborated from two independent directions. Binance's own Privacy Notice (section 9) states that personal data of Mandarin or Chinese speaking users may be accessed by Customer Support located in China. Independently of that disclosure, the binary integrates SensorsData (Sensors Data Co., Ltd, Beijing), whose ContentProvider is instantiated by the operating system at process start, before any consent screen can render (H1), and JPush/Jiguang, which ships four components that any other app on the same device can reach without holding a permission (H2).

Binance's current posture also contains genuine strengths, recorded in full below: cleartext traffic is blocked app-wide, no extractable hardcoded key was found across all 22 dex files, no Firebase auto-initialization provider exists, background location is not requested, and a five-vendor KYC stack, Travel Rule address states and a reused jurisdictional-exit architecture are visibly engineered. The EU MiCA gating architecture is real and substantial; whether it is enforced live for EU accounts could not be determined from a static pass, so the verdict is PARTIAL.

RFI-IRFOS put three yes or no questions to Binance on 2 July 2026 and repeated them on 27 July, 9 August and 31 August. The Data Protection Office answered each delivered message with an automated acknowledgment, and once with a templated redirect to the Bug Bounty Program that also invited a data-protection submission, which RFI-IRFOS answered the same day by confirming in writing that this is a data protection matter. After 107 days and an embargo that passed 17 days ago, none of the three questions has been answered and H1 and H2 remain unaddressed on the merits. This report is the public record of that state.

ID	Severity	Title
H1	HIGH	SensorsData (China) behavioral-analytics Content-Provider initializes before any consent screen can render
H2	HIGH	JPush/Jiguang: two exported services and two exported content providers without any permission guard
M1	MEDIUM	Chinese-vendor SDK inventory: JPush/Jiguang and SensorsData confirmed; Nezha and Agora resolved and dropped
L1	LOW	No TLS certificate pinning; cleartext correctly blocked app-wide; no user-CA trust in the release path

Subject & Operator Context

Binance is operated through the Nest group of entities registered in the Abu Dhabi Global Market (Nest Exchange Limited, Nest Trading Limited, Nest Clearing and Custody Limited), with VeraSafe Ireland Ltd appointed as the GDPR Article 27 representative in the European Union. No EU main establishment is identified in the privacy notice, so the Austrian DSB, as the supervisory authority of the initiating researcher, and the EDPS were copied throughout. The app serves a global trading, payments, social content and live-streaming user base and handles KYC documents, biometric liveness data, card payments and sanctions screening results. A platform handling this class of data and publishing a China-based customer-support access path in its own privacy notice raises the stakes of each pre-consent and exposure finding beyond what the same findings would mean for a smaller operator.

Engagement Summary

RFI-IRFOS analyzed com.binance.dev v3.16.7 on 2 July 2026 using apktool (manifest and resources, memory-safe pass without baksmali), raw string extraction across all 22 classes*.dex files, an independent aapt2 xmltree and badging cross-check of the manifest, and a cross-reference against Binance's live Privacy Notice dated 5 January 2026. base.apk SHA-256: ae09cdf34608cec818e6d6e37b82e5fdc828060056cd0b223ab49a5899e40318. No Binance servers, accounts or production infrastructure were probed or accessed.

The initial disclosure went out the same day to dpo@binance.com, the contact the privacy notice names for data protection (section 16), and to pr@binance.com, with the Austrian DSB and the EDPS in copy, fixing a 90-day embargo of 30 September 2026. The disclosure listed H1 and H2 and put three yes or no questions on SensorsData awareness, the Article 28 processor agreement and the Article 35 DPIA.

A pass of this size left R2 follow-ups open and documented in the Residual Risk section. They include a live geolocated EU account test for the MiCA verdict, a network capture to determine where SensorsData's pre-consent data goes, a cross-app access test against the four exported JPush components, and desk research on the 'local regulated exchange entity' placeholder in the controller table.

Findings

H1: SensorsData (China) behavioral-analytics ContentProvider initializes before any consent screen can render

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 - pre-consent initialization of a China-headquartered analytics vendor, corroborated by Binance's own privacy notice

```
<provider android:authorities="com.binance.dev.SensorsDataContentProvider"
    android:enabled="true" android:exported="false"
    android:name="com.sensorsdata.analytics.android.sdk.data.
    SensorsDataContentProvider"/>
<meta-data android:name="com.sensorsdata.analytics.android.MainProcessName" android:
    value="com.binance.dev"/>
<meta-data android:name="com.sensorsdata.analytics.android.version" android:value
    ="0.2.10"/>
<!-- res/values/strings.xml: sensors_analytics_remote_config = collection-control
    fetch at runtime -->
```

Personal data of Mandarin or Chinese speaking users may be accessed by Customer Support located in China, where the relevant users seek local language support. Any remote access from China to user data is carried out in accordance with necessary safeguards which ensure an adequate level of protection for personal data.

Impact: AndroidManifest.xml declares com.sensorsdata.analytics.android.sdk.data.SensorsDataContentProvider in the main process. Android instantiates a declared provider during Application process creation, before the first Activity and therefore before any consent screen is displayed; exported=false limits access by other apps and does not delay the provider's own onCreate(). SensorsData is a third-party behavioral-analytics product from Sensors Data Co., Ltd (Beijing), and the app fetches its collection-control configuration at runtime (string sensors_analytics_remote_config). Binance's own Privacy Notice, section 9, states: 'Personal data of Mandarin or Chinese speaking users may be accessed by Customer Support located in China'. Observed fact: the provider auto-initializes pre-consent and Binance discloses China-based access to user data for customer support. Open question put to Binance: whether SensorsData-collected data is among the data accessed from China or leaves Binance-controlled infrastructure. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the pre-consent initialization sits in a financial application with biometric KYC data and because Binance's own notice independently confirms a China data-access path, a combination the CVSS technical scope does not capture.

H2: JPush/Jiguang: two exported services and two exported content providers without any permission guard

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 5.5 - four cross-app-reachable components from a China-origin push vendor, no android:permission on any of them

```
E: provider cn.jiguang.privates.core.service.DataProvider
  exported=true process=:push authorities=com.binance.dev.DataProvider [no
  android:permission]
E: service cn.jpush.android.service.PushService exported=true [no android:
  permission]
E: service cn.jpush.android.service.DaemonService exported=true [no android:
  permission]
  intent-filter action=cn.jpush.android.intent.DaemonService category=com.binance.dev
E: provider cn.jpush.android.service.DownloadProvider exported=true
  authorities=com.binance.dev.DownloadProvider [no android:
  permission]
```

```
JIGUANG_PRIVATES_APPKEY    = "[REDACTED IN PUBLIC REPORT -- disclosed privately to
  Binance in R1]"
JIGUANG_PRIVATES_CHANNEL   = "developer-default"
```

Impact: The authoritative aapt2 dump of the production manifest shows four components exported=true with no android:permission attribute: cn.jiguang.privates.core.service.DataProvider (process :push), cn.jpush.android.service.PushService, cn.jpush.android.service.DaemonService and cn.jpush.android.service.DownloadProvider. Any other app installed on the same device can send intents to the two services and query the two content providers, subject only to the validation inside JPush's closed-source code. The JPush app key is hard-coded in the manifest (JIGUANG_PRIVATES_APPKEY, value redacted in this public report and disclosed to Binance in R1). The end-to-end impact of the exposure (data read, forced download, push spoofing, denial of service) was not exercised, because the JPush internals were not decompiled in this memory-safe pass; the finding rests on the observed reachability. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.5 to HIGH because four unguarded components from a China-origin vendor sit inside an application that handles KYC documents and trading credentials, and because the same vendor class is the subject of the China data-access disclosure in H1.

M1: Chinese-vendor SDK inventory: JPush/Jiguang and SensorsData confirmed; Nezha and Agora resolved and dropped

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N, 4.5 - two third-party China-origin SDKs in the binary; the transfer destination of their specific data flows is not verified

Impact: Two actively integrated, third-party, China-origin SDKs are confirmed: JPush/Jiguang (push notifications, H2) and SensorsData (behavioral analytics, H1). Two earlier suspects were resolved and removed from the list. com.nezha.android.* is first-party Binance code, an in-house mini-program hybrid container that sits in Binance's own package namespace (com.binance.android.nezha.api.view.CommonMPViewBasedFragment). io.agora rtc2.* is Agora, Inc. (NASDAQ: API, Santa Clara), wired to the in-app live-streaming feature. Ruled out as false positives: com.tencent.mm appears only in a queries block (a share-to-WeChat capability check), and the Huawei App Market referrer permission is attribution plumbing. This entry exists to give the complete SDK picture. It records that the Article 28 processor relationship and the Chapter V transfer basis for these two vendors are not documented in the privacy notice at vendor level, which is the substance of question 2.

L1: No TLS certificate pinning; cleartext correctly blocked app-wide; no user-CA trust in the release path

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 3.1 - no pinning means a compromised or coerced system CA could intercept traffic undetected

```
<network-security-config>
  <debug-overrides>
    <trust-anchors>
      <certificates src="system" />
      <certificates src="user" />
    </trust-anchors>
  </debug-overrides>
  <base-config cleartextTrafficPermitted="false" />
</network-security-config>
```

Impact: The network security config sets cleartextTrafficPermitted=false at base-config with no domain-config override anywhere, the strongest cleartext posture short of pinning. No pin-set is configured for any domain, so the app trusts whatever the system CA store trusts. User-installed CAs are trusted only inside debug-overrides, which applies to debuggable builds and not to the shipped release. Absence of pinning alone, without a demonstrated interception path, does not constitute demonstrated impact, so the finding stays LOW. It is recorded because of the transaction value this specific application carries.

Impact Analysis

H1 and H2 describe the same vendor class from two directions. H1 is a data-collection decision: a third-party analytics SDK from a Beijing vendor starts before consent is possible, in an app whose own privacy notice states that China-located staff can access user data for a defined purpose. H2 is an exposure decision: four components of a China-origin push vendor are reachable by any app on the device without a permission. Neither finding on its own proves exfiltration. Together they describe a real, self-disclosed China data-access nexus sitting behind SDK integrations with a weak cross-app posture, and the three questions put to Binance ask precisely for the documents that would close that gap: awareness, an Article 28 agreement that covers the China access, and an Article 35 DPIA for biometric KYC, automated sanctions and PEP screening and automated account locking.

The case is also an example of how strong parts and weak parts coexist in one application. Cleartext blocking, absence of extractable secrets, foreground-only location and the isolation of the Onfido KYC components show an engineering team that knows the checklist. The open items are the ones that need a legal and vendor-management answer, which is why the questions went to the Data Protection Office.

The Complete Chain: Seven Messages Sent, Seven Automated Responses, Zero Answers

2 July 2026: RFI-IRFOS sends the original disclosure to dpo@binance.com and pr@binance.com, with the DSB and the EDPS in copy, embargo 30 September 2026. Within seconds two automated messages arrive: the PR team's auto-reply (for media enquiries only) and the Data Protection Office's standard acknowledgment.

6 July 2026 (day 4): follow-up reporting four days with no reply. Gmail rejects the message for all four recipients (status 5.7.1); it never reaches Binance.

7 July 2026: the Data Protection Office sends a different templated message. It states that the enquiry 'falls outside the scope of the DPO Team's assistance' because the channel is 'exclusively dedicated to Privacy Rights-related queries', suggests the Binance Bug Bounty Program on Bugcrowd, and invites a reply with detail 'if your enquiry is specifically a data protection issue'. RFI-IRFOS replies the same day confirming that it is specifically a data protection issue. Gmail again rejects that message for all four recipients (5.7.1).

27 July 2026 (subject 'prior send bounced, resending'): the three questions go out again to dpo@binance.com, CC pr@binance.com, the EDPS and the DSB. The message is accepted and the standard acknowledgment returns within seconds.

9 August 2026: third identical acknowledgment after another follow-up.

24 August 2026: follow-up titled 'Your Own Data Protection Office'. Fourth identical acknowledgment returns.

31 August 2026: final follow-up, seven days after the fourth acknowledgment and sixty days after R1, listing the chronology and repeating the three questions. A further identical acknowledgment returns.

30 September 2026: embargo reached. Correspondence record: 7 messages sent (5 delivered, 2 rejected by Gmail), 7 automated or templated messages received, 1 redirect to a bug-bounty program, 0 of 3 questions answered.

17 October 2026: this report publishes, 17 days after the embargo and 107 days after the original disclosure. H1 and H2 are treated as unaddressed on the merits.

Disclosure Timeline & Outcome

2026-07-02 Initial disclosure (R1) to dpo@binance.com and pr@binance.com, DSB and EDPS in copy. Embargo fixed at 2026-09-30. PR auto-reply and DPO acknowledgment arrive the same minute.

2026-07-06 Follow-up rejected by Gmail for all four recipients (5.7.1). Not delivered.

2026-07-07 Templated DPO message: out of DPO scope, Bugcrowd program suggested, data-protection submission invited. RFI-IRFOS confirms in writing that this is a data-protection matter. That reply is rejected by Gmail for all four recipients (5.7.1). Not delivered.

2026-07-27 Resend of the follow-up and the three questions, accepted. Standard DPO acknowledgment returns.

2026-08-09 Follow-up, accepted. Third identical acknowledgment.

2026-08-24 Follow-up titled 'Your Own Data Protection Office', accepted. Fourth identical acknowledgment.

2026-08-31 Final follow-up with the full chronology, accepted. Further identical acknowledgment.

2026-09-30 Embargo date reached. Correspondence record: 7 messages sent, 2 rejected by Gmail, 7 automated or templated replies, 0 questions answered.

2026-10-17 This report published, 17 days after embargo, 107 days after original disclosure. H1 and H2 unaddressed on the merits.

MiCA / EU Jurisdiction-Gating Thesis: Test Result PARTIAL

What was tested: whether the app contains genuine client-side architecture for the EU MiCA exit-only restriction (stop onboarding, stop new spot orders, stop deposits, stop Earn and staking, keep withdrawals open) or whether the restriction exists only in public statements.

Evidence found: an EU-specific exit-only banner (string `compliance_content_test`) whose wording tracks the ESMA requirement almost word for word; the identical mechanism already proven in production for the 2023 US exit (us_compliance_banner and a family of risk_user_restricted_us strings); a dedicated 'EU Futures' regulated product silo with 26 or more eu_kyc strings, mandatory proof of address, a suitability questionnaire with a cooling-off period and explicit KYB and broker exclusions; MiCA-specific product restrictions (alpha_mica_trading_unavailable and a futures_mica_switch_credits_mode family forcing EU futures accounts into a reduced-risk Credits Trading Mode); a server-populated, client-consumed EU country list as a first-class field (FiatConfig.euCountryList); and a distinct sanctions-triggered withdrawal-interception path segmented by VIP tier. The privacy notice names the UN sanctions list, the US ITA Consolidated Screening List and SEC EDGAR as screening sources, which aligns with the binary and is recorded as agreement between policy and code.

Open items: the controller table lists France under a generic row with 'the local regulated exchange entity' as a placeholder, while Poland and Belgium name a specific entity (Binance Poland sp. z o.o.). This asymmetry was not resolved because the hyperlink was not followed. No Earn or staking EU-restriction string was found, which does not prove the product is

unrestricted. The client binary cannot show that the machinery is switched on for real EU accounts, nor which signal (IP, KYC country, GPS or locale) drives the decision.

Conclusion: the thesis that the restriction is cosmetic is not supported by the evidence. The thesis that it is fully enforced is not confirmed. Verdict PARTIAL, pending a live geolocated account test.

Informational: Credential Hygiene Result

The `google_api_key` and `google_crash_reporting_api_key` resource values do not match the standard Alza Firebase key format, consistent with build-time obfuscation of sensitive resource values. Patterns searched across `strings.xml` and all 22 dex string dumps returned zero matches: the Firebase/Google key format, AWS access key IDs, Stripe-style secret key prefixes, and literal `app_secret` or `client_secret` assignments. The only secret-named string resources are UI copy for MPC wallet key display. `google_app_id` and the OAuth client ID are public by Google's design. No `FirebaseInitProvider` is declared anywhere in the manifest, and Crashlytics collection is disabled by meta-data. Honest limit: the deobfuscation routine for `google_api_key` was not located, so whether the runtime value is a live key was not tested and remains an R2 item. This is a positive result and carries no severity.

What Binance Got Right

`cleartextTrafficPermitted=false` at base-config with no domain-level carve-outs. No plaintext-extractable Firebase or Google key and no other hardcoded secret across `strings.xml` and all 22 dex files. No `FirebaseInitProvider`, and Crashlytics collection disabled by meta-data. A `CCESS_BACKGROUND_LOCATION` is not requested, so location access is foreground-only. `allowBackup=false` and `extractNativeLibs=false`. A five-vendor, region-aware KYC stack (Onfido, Sumsub, Persona, Liquidinc, Uqudo) with Onfido isolated in its own `:onfido_process`, all providers `exported=false`, activating only during a user-initiated flow. FATF Travel Rule address states (declared, pending, unverified, verified) in the client. CardinalCommerce 3-D Secure for card payments. `DETECT_SCREEN_CAPTURE` together with anti-overlay dialogs as a defense against banking-trojan overlay attacks. A current, detailed privacy notice with named legal bases per purpose, an explicit Article 27 representative and a named DPO contact. A previously battle-tested jurisdictional-exit architecture reused from the 2023 US exit. This list is part of the public record because an honest report records strengths next to gaps.

Data Protection Article by Article

Art. 6 and Art. 7 GDPR: H1's pre-consent ContentProvider initialization means any consent collected later cannot retroactively authorize collection that started at process creation. The legal basis for that collection was asked about in question 1 and in R1.

Art. 28 GDPR: Sensors Data Co., Ltd and Jiguang act as processors or sub-processors in the binary. Whether a documented processing agreement exists, and whether it covers the China remote access disclosed in section 9 of the privacy notice, is question 2. It remains unanswered.

Art. 32 GDPR: H2's four exported and unguarded components are a technical-measure question under Art. 32(1) regardless of what the JPush internals do with the intents they receive.

Art. 33 GDPR: if either H1 or H2 qualifies as a personal data breach, the 72-hour clock runs from awareness. Question 1 asks whether Binance is aware. The supervisory authority copies in this correspondence have had full visibility since 2 July 2026.

Art. 35 GDPR: biometric KYC data, automated sanctions and PEP screening and automated account locking are high-risk processing. Whether a DPIA exists and has reached the DPO is question 3. It remains unanswered.

Art. 44 to 46 GDPR: the China-located customer-support access in section 9 is a third-country transfer. Safeguards are asserted in the notice; the instrument is not named.

Regulatory Landscape & Fine Exposure

The data controllers are registered in the Abu Dhabi Global Market and no EU main establishment is identified in the privacy notice. VeraSafe Ireland Ltd is appointed as Article 27 representative, which does not create a main establishment for Article 56 purposes. The Austrian DSB and the EDPS received the correspondence from the first message. Any supervisory authority in a member state where affected users reside may independently assert jurisdiction, and the MiCA gating questions fall under the national competent authorities and ESMA guidance in parallel to GDPR.

Art. 83(5) GDPR: fines up to EUR 20,000,000 or 4% of worldwide annual turnover apply to violations of Art. 5, 6, 7 and 44 to 46. H1 and the China-access disclosure implicate this tier.

Art. 83(4) GDPR: fines up to EUR 10,000,000 or 2% of worldwide annual turnover apply to violations of Art. 25, 28, 32 and 35. H2, the processor-agreement question and the DPIA question implicate this tier.

This report states exposure categories; it does not predict any authority's decision.

Indicators of Compromise

All findings derive from static analysis of com.binance.dev v3.16.7 as published on Google Play, analyzed 2026-07-02. base.apk SHA-256: ae09cdf34608cec818e6d6e37b82e5fdc828060056cd0b223ab49a5899e40318. Components of interest: com.sensorsdata.analytics.android.sdk.data.SensorsDataContentProvider; cn.jiguang.privates.core.service.DataProvider; cn.jpush.android.service.PushService, DaemonService and DownloadProvider. No Binance servers, accounts or production infrastructure were probed or accessed.

Residual Risk & Recommendations

H1: gate SensorsData initialization behind a confirmed consent decision so the provider does not run at process creation; document the Article 6 basis; state in the privacy notice whether SensorsData data is among the data accessible from China.

H2: add android.permission (signature level) to the four exported JPush/Jiguang components or set exported=false where the vendor contract allows; rotate the Jiguang app key if exposure is a concern.

M1: name Sensors Data Co., Ltd and Jiguang as processors in the privacy notice and document the Article 28 agreements and the Chapter V transfer instrument.

L1: evaluate certificate pinning for the trading and KYC endpoints given the transaction value.

Question 3: if no DPIA exists for biometric KYC, automated sanctions and PEP screening and automated account locking, conduct one and ensure it reaches the DPO.

Process-level: a data-protection contact that answers a security disclosure with a standard acknowledgment five times needs an internal route to a person who can read it.

Open R2 items for RFI-IRFOS: live geolocated EU account test (MiCA verdict), network capture of SensorsData traffic, cross-app access test against the exported JPush components, desk research on the 'local regulated exchange entity' placeholder, scoped decompile of com.face.csg.lv5.sdk and com.shield.ptr, deobfuscation of google_api_key, and a live Earn and staking EU-eligibility check.

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

com.binance.dev as published on Google Play, analyzed 2026-07-02, using publicly available tools (apktool, aapt2, string extraction). No Binance servers, accounts or production infrastructure were probed or accessed. Technical evidence is archived under chain of custody and will be provided to the competent supervisory authority on request. Research conducted under GDPR Art. 89 (scientific research exemption), ISO/IEC 29147 (coordinated disclosure standard), and the Austrian Federal Constitutional Law Art. 17 (freedom of research). REF BINANCE-2026-R1-001.