Coordinated Security & Privacy Disclosure, Final Report

Plus500 for Android (com.Plus500, v26.6.0, versionCode 143328)

Eight written notices, ninety-one days, two identical portal-redirect auto-replies, zero human replies

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SEVEN FINDINGS UNADDRESSED AFTER EIGHT NOTICES

Target	Plus500 group (Plus500CY, Plus500EE, Plus500SEY, Plus500Gulf)
Product audited	Plus500 for Android, com.Plus500, v26.6.0, versionCode 143328
Disclosure reference	REF PLUS500-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 sixteen development/staging hostnames in the production Network Security Config with cleartext permitted and zero certificate pinning on live trading traffic, CVSS v4.0 8.6, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Plus500 Android application and identified three CRITICAL and four HIGH findings: an unrotated Firebase API key hardcoded in the shipped APK, sixteen development and staging server hostnames (devbox1.plus500.com through devbox16.plus500.com, plus dev.plus500.com and mevideo.local) present in the production Network Security Configuration with cleartextTrafficPermitted=true and no production domain-config or certificate pinning at all, leaving trading API traffic, balances, orders, and positions, without protection, an in-app account-transfer flow that offers EU and Australian retail clients facing the ESMA/CySEC 1:30 leverage cap a transfer to Plus500SEY (Seychelles, no investor compensation scheme, 1:300 leverage) or Plus500Gulf (UAE CMA, 1:300, no investor compensation), a ContentSquare session-replay integration (2,168 smali classes) capturing bitmap screenshots of live account balances, open-position profit and loss, and order-entry touch behavior, an AppsFlyer ad-attribution SDK whose own code authored the app's cloud-backup exclusion rules, protecting only AppsFlyer's own data rather than the user's, a Braze CRM integration (1,272 smali classes) processing a full behavioral event stream for market-movement alerts and deposit-nudge campaigns with no disclosed processor relationship, and an AU10TIX biometric KYC integration processing facial images with no cited Art. 46 adequacy documentation for the transfer to Israel.

Across eight written notices over ninety-one days, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde, CERT.at, the UK ICO, and CySEC, the only inbound correspondence was two identical automated support-portal redirect auto-replies from support@plus500.com, each directing RFI-IRFOS to a customer data-request web form rather than engaging with the disclosure. privacy@, security@, and legal@plus500.com all bounced as nonexistent addresses on the first attempt. No substantive human reply was ever received. None of RFI-IRFOS's three standing questions, on the Art. 6/7 legal basis for ContentSquare's screen capture of live trading positions, DPO awareness independent of the automated replies, or a documented Art. 35 DPIA covering AU10TIX, ever received an answer.

Scope: Static analysis of the publicly downloaded production Plus500 Android APK (v26.6.0), on an authorized test device, only. No Plus500 account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to privacy@plus500.com (bounced) and DPO@plus500.com, cc security@plus500.com (bounced) and legal@plus500.com (bounced), bcc the Austrian Datenschutzbehoerde, CERT.at, the UK ICO, and CySEC. Across eight written notices over ninety-one days, the only inbound correspondence was two identical automated support-portal redirect replies; no substantive human reply was ever received.

ID	Severity	Title
C1	CRITICAL	Hardcoded, unrotated Firebase API key and project configuration in the production APK

ID	Severity	Title
C2	CRITICAL	Sixteen development/staging hostnames in the production Network Security Config, cleartext permitted, no certificate pinning
C3	CRITICAL	In-app flow routes EU/AU retail clients to a Seychelles entity offering 1:300 leverage, bypassing the ESMA 1:30 cap
H1	HIGH	ContentSquare session-replay SDK captures bitmap screenshots of live trading positions and balances
H2	HIGH	AppsFlyer's own SDK authored the app's cloud-backup exclusion rules
H3	HIGH	Braze CRM processes the full behavioral event stream for trading engagement nudges, undisclosed as processor
H4	HIGH	AU10TIX biometric KYC processor undisclosed, no cited Art. 46 adequacy documentation

Subject & Operator Analysis

Plus500 operates through several group entities depending on client jurisdiction: Plus500CY (Cyprus, regulated by CySEC), Plus500EE (Estonia, regulated by the Estonian FSA), Plus500SEY (Seychelles, unregulated for EU purposes), and Plus500Gulf (UAE, regulated by the CMA).

Findings

C1: Hardcoded, unrotated Firebase API key and project configuration in the production APK

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

res/values/strings.xml contains google_api_key/google_crash_reporting_api_key AIzaSyC3IoLjnd-pmnsPBwWmbiNPIA_jMo2tbjE, Firebase project api-project-731586421521, database URL https://api-project-731586421521.firebaseio.com, a default_web_client_id, and a Facebook client token. The legacy api-project-<number> naming convention indicates this credential was never rotated since the initial Firebase integration.

No reply of any kind, substantive or otherwise, addressed this finding across eight notices.

Impact: A production Firebase project's attack surface, apparently unrotated since initial integration, 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: Sixteen development/staging hostnames in the production Network Security Config, cleartext permitted, no certificate pinning

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

res/xml/network_security_config.xml ships devbox1.plus500.com through devbox16.plus500.com, plus dev.plus500.com and mevideo.local, with cleartextTrafficPermitted=true (a leading-space formatting bug in these entries may cause the Android NSC parser not to match them as intended). No base-config and no production domain-config exist, meaning trading API traffic, balances, orders, and open positions, has zero certificate pinning.

No reply of any kind addressed this finding.

Impact: Live trading data, account balances, orders, and positions, is transmitted with no certificate pinning and is susceptible to interception on any untrusted network.

Fix: Remove all development and staging hostnames from the production configuration, add an explicit production domain-config, and implement certificate pinning for trading API traffic.

C3: In-app flow routes EU/AU retail clients to a Seychelles entity offering 1:300 leverage, bypassing the ESMA 1:30 cap

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

Verbatim strings strACCOUNT_TRANSFERED_DEFAULT_AU_SEY and strACCOUNT_TRANSFERED_TO_NEW_DEFAULT_OPERATOR_DFSA_TO_CMA present a live, templated in-app consent flow offering clients facing the ESMA/CySEC 1:30 leverage cap a transfer to Plus500SEY (Seychelles, no investor compensation scheme, 1:300 leverage) or Plus500Gulf (UAE CMA, 1:300, no investor compensation), referencing the live domain plus500.com.sc.

No reply of any kind addressed this finding.

Impact: Retail clients facing an EU investor-protection leverage cap are offered a templated pathway to an entity outside that protection regime and without an investor compensation scheme.

Fix: Remove or substantially restrict the templated cross-entity transfer flow for EU/AU retail clients subject to the ESMA leverage cap.

H1: ContentSquare session-replay SDK captures bitmap screenshots of live trading positions and balances

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

2,168 smali files under com/contentsquare/, including viewbitmap/BitmapInstantiable and ScreenViewTracker, capture account balance/equity screens, open-position profit and loss, and touch behavior during order entry, transmitted to ContentSquare SAS in France.

No reply of any kind addressed the Art. 6/7 legal basis for this capture.

Impact: Live account balances and open-position data may be captured as screen-replay bitmaps and transmitted to a third-party processor with no confirmed matching disclosure.

Fix: Exclude balance, position, and order-entry screens from ContentSquare's session-replay capture, or obtain a specific consent covering it.

H2: AppsFlyer's own SDK authored the app's cloud-backup exclusion rules

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

457 smali files implement AppsFlyer, and the manifest's android:dataExtractionRules= "@xml/appsflyer_data_extraction_rules" shows the app's cloud-backup exclusion configuration was written by the AppsFlyer SDK itself, protecting only AppsFlyer's own data rather than the user's broader trading data.

No reply of any kind addressed this finding.

Impact: The app's own device-to-device and cloud backup exclusion policy is effectively delegated to a third-party ad-attribution vendor rather than defined by the app operator for the user's benefit.

Fix: Author a first-party data_extraction_rules.xml covering all sensitive trading data, not only AppsFlyer's own data.

H3: Braze CRM processes the full behavioral event stream for trading engagement nudges, undisclosed as processor

---

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

1,272 smali files implement Braze; Braze Inc. (New York) receives market-movement alerts, deposit nudges, and re-engagement campaign triggers derived from the user's trading behavior.

No reply of any kind addressed this finding.

Impact: A full behavioral trading-event stream is transmitted to a named US processor with no confirmed matching Art. 13(1)(e) disclosure.

Fix: Name Braze explicitly as a processor of trading-behavior data in the privacy policy.

H4: AU10TIX biometric KYC processor undisclosed, no cited Art. 46 adequacy documentation

---

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

The strAU10TIX_CONSENT_POPUP_CONTENT consent text confirms processing of facial images and biometric data by AU10TIX Ltd (Tel Aviv, Israel). An FCA-specific consent variant offers a manual-verification opt-out not consistently present in other jurisdictions.

No reply of any kind confirmed whether an Art. 46 adequacy or transfer mechanism covers this specific processor and data category.

Impact: Biometric facial data may be transferred to an Israeli processor for identity verification with no cited Art. 46 transfer mechanism, and the opt-out available to some jurisdictions is not consistently offered to others.

Fix: Cite the specific Art. 46 transfer mechanism covering AU10TIX, and offer the manual-verification opt-out consistently across jurisdictions.

Two Portal Redirects, Zero Substance

The only inbound correspondence this case produced was two identical automated replies from support@plus500.com, both directing RFI-IRFOS to a customer personal-data-request web form rather than engaging with the disclosure. privacy@, security@, and legal@plus500.com all bounced as nonexistent addresses on the first attempt. Eight notices over ninety-one days produced no substantive human reply of any kind.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Unrotated Firebase key hardcoded in the production APK
C2	GDPR Art. 32(1)(a)	Development hosts and no certificate pinning on live trading traffic
C3	Investor protection (ESMA/CySEC leverage rules)	Templated flow routing EU/AU clients around the leverage cap
H1	GDPR Art. 6(1), Art. 7	Session-replay capture of live balance and position data
H2	GDPR Art. 32	Third-party-authored backup-exclusion policy protecting only vendor data
H3	GDPR Art. 13(1)(e)	Undisclosed behavioral-data processor
H4	GDPR Art. 9, Art. 46	Undocumented transfer mechanism for biometric KYC data

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@plus500.com (bounced) and DPO@plus500.com; security@ and legal@ bounce; automated portal-redirect autoreply from support@plus500.com
2026-06-28	Follow-up; privacy@ and security@ bounce again; second identical automated autoreply
2026-07-23/24	Follow-up to DPO@plus500.com, three questions restated, Austrian DSB in cc
2026-09-03	Follow-up, '74 Days of Silence, 16 Days Until Public Disclosure'
2026-09-12	Follow-up, '83 Days, One Automated Portal Redirect, Seven Days Until Public Disclosure'
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Remove development and staging hostnames from the production Network Security Config and implement certificate pinning for trading traffic.
- Remove or substantially restrict the templated cross-entity transfer flow offered to EU/AU retail clients subject to the ESMA leverage cap.
- Exclude balance, position, and order-entry screens from ContentSquare's session-replay capture.
- Name Braze and AU10TIX explicitly as processors, with the applicable legal basis and transfer mechanism for each.
- Rotate the exposed, unrotated Firebase key.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. GDPR Art. 6, 7, 9, 13, 25, 32, 46. REF PLUS500-2026-R1.