Coordinated Privacy Disclosure, Final Report

Bitpanda Android (com.bitpanda.bitpanda)

Bitpanda GmbH, Vienna, Austria, MiFID II regulated, supervised by the FMA

CS-DEFLECT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ONE DAY AFTER THE STATED 24 SEPTEMBER EMBARGO, EIGHT MESSAGES, TWO IDENTICAL AUTO-REPLY TICKETS, ZERO SUBSTANTIVE REPLY

Target	Bitpanda, an Austrian crypto trading platform
Package	com.bitpanda.bitpanda, version 3.26.0
Operator	Bitpanda GmbH, Vienna, Austria
Initial Disclosure	2026-06-26
Stated Embargo	2026-09-24, as restated directly to the target in later correspondence, superseding the 2026-09-19 date given in the initial disclosure
Report Published	2026-09-25, one day after the stated date
Regulators	Austrian DSB, Austrian FMA (MiFID II supervisor), CERT.at, EDPS
Total Outbound Messages	8, across 78 days, all via privacy@bitpanda.com; info@bitpanda.com and eric.demuth@bitpanda.com were blocked by an enterprise mail policy from the first send onward.
Inbound Replies	2 automated Zendesk support-ticket acknowledgments (tickets 3599061 and 3658413), addressing none of the six findings. No substantive human reply was ever received.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 26 June 2026, RFI-IRFOS disclosed to Bitpanda GmbH, an Austrian crypto trading platform regulated under MiFID II and supervised by the FMA, that its Android app initializes Firebase Analytics with directBootAware=true and a RECEIVE_BOOT_COMPLETED receiver, meaning the SDK begins running in the before-first-unlock phase immediately after a device reboot, before the user has had any opportunity to provide consent.

The most structurally significant finding concerns identity verification. The app embeds Fourthline, a Dutch KYC vendor, running selfie liveness capture and NFC passport chip reading, both Art. 9(1) GDPR special-category biometric processing. A second, separate KYC SDK, IDnow, runs in parallel in the same binary, meaning two independent biometric identity pipelines process the same user with no documented justification for why both are necessary. Braze, a New York-based customer engagement platform with an active location module, separately receives trading behavior and portfolio-interest data linked to a hardware advertising ID, a transfer of financial behavioral data to US infrastructure on a regulated investment platform.

Three further findings, an Adjust attribution SDK that links advertising campaign data to in-app trading events, a Datadog real-user-monitoring ContentProvider that auto-initializes and transmits session data including financial UI interactions to US infrastructure, and the same pre-consent Firebase initialization named above, round out the six-finding disclosure. Genuine positives are worth naming: allowBackup is false, cleartext traffic is blocked, and the app ships a correctly implemented biometric login authenticator, the compliance gap sits specifically in the third-party SDK layer and the boot-time initialization sequence, not in Bitpanda's own authentication or transaction code.

Eight messages were sent across 78 days, all delivered to privacy@bitpanda.com, cc'ing the Austrian DSB and EDPS on later rounds; info@bitpanda.com and eric.demuth@bitpanda.com were blocked by an enterprise mail policy from the first send onward. The only inbound replies were two identical automated Zendesk support-ticket acknowledgments (tickets 3599061 and 3658413), addressing none of the six findings, none of which involved a support-ticket-appropriate question. The embargo, restated directly to the target as 24 September 2026 in later correspondence, elapsed one day before this report and closure notice publish.

Scope: Root-level static analysis of the production Bitpanda Android application (com.bitpanda.bitpanda, version 3.26.0), pulled from Google Play and reviewed on 26 June 2026. No account was created, no KYC flow was completed, and no interaction with Fourthline's, IDnow's, Braze's, Adjust's, or Datadog's backend infrastructure was performed.

Disposition

Six findings were disclosed on 26 June 2026, re-scored under CVSS v4.0. Two correct to HIGH on their own computed bands: the Fourthline biometric NFC passport and selfie-liveness pipeline, an Art. 9 special-category-data finding running in parallel with a second KYC SDK with no documented DPIA justification for the dual pipeline, and Braze's transfer of financial transaction and location data, linked to a hardware advertising ID, to US infrastructure. Pre-consent Firebase initialization with a directBootAware provider and BOOT_COMPLETED receiver, the Adjust attribution SDK linking ad campaigns to trading behavior, and Datadog's auto-initializing US-bound session monitoring all correct to MEDIUM. Eight messages were sent across 78 days. The only inbound replies were two identical automated Zendesk support-ticket acknowledgments, addressing none of the six findings.

ID	Severity	Title
C1	MEDIUM	Firebase Initializes Before Device Unlock, Before Any Consent Screen
C2	HIGH	Dual Biometric KYC Pipelines With No Documented DPIA Justification
C3	HIGH	Braze Receives Trading Behavior and Location Data Linked to a Hardware Ad ID
H1	MEDIUM	Attribution SDK Links Advertising Campaigns to Trading Behavior
H2	MEDIUM	Datadog Session Monitoring Auto-Initializes and Transfers Data to the US

Subject & Operator Analysis

Bitpanda GmbH is an Austrian crypto trading platform regulated under MiFID II and supervised by the Austrian FMA. As a MiFID II supervisor, the FMA has independent jurisdiction over operational and compliance risk in regulated investment services, separate from the DSB's GDPR jurisdiction.

Genuine positives are worth naming. allowBackup is correctly set to false, and usesClearte xtTraffic is correctly set to false, the right defaults for a financial application. The app ships a fingerprint and biometric login authenticator appropriate for a financial platform, and the core MFA architecture is sound. The issues in this report sit specifically in the third-party SDK layer and the boot-time initialization sequence, not in Bitpanda's own authentication or transaction code.

Eight Messages, Two Identical Auto-Reply Tickets, Zero Substantive Reply

This case's correspondence record involved two identical automated responses. privacy@bitpanda.com's Zendesk-integrated support system returned a templated ticket acknowledgment on the same day as the initial disclosure (ticket 3599061) and again after the 27 July follow-up (ticket 3658413), both addressing none of the six technical findings. Five further follow-up messages through 12 September 2026 restated the same three yes/no questions repeatedly, receiving no reply of any kind, not even a further automated acknowledgment. info@bitpanda.com and eric.demuth@bitpanda.com were both blocked outright by an enterprise mail policy from the first send onward.

Findings

C1: Firebase Initializes Before Device Unlock, Before Any Consent Screen

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.

FirebaseInitProvider is declared with directBootAware="true" and initOrder=100, alongside a RECEIVE_BOOT_COMPLETED permission and an ML Kit provider at initOrder=99. directBootAware means Firebase initializes in the before-first-unlock phase immediately after device boot, before the user has had any opportunity to provide consent. A hardcoded Firebase API key, database URL, and storage bucket are additionally present in the production binary.

```
FirebaseInitProvider: initOrder=100, directBootAware=true
MlKitInitProvider: initOrder=99
google_api_key: AIzaSyBdQdwgjFgqi6cJFfhVA8jhyRaL2xDYmyQ
firebase_database_url: https://bitpanda-b6b89.firebaseio.com
```

Impact: Tracking infrastructure is active on a cold device before any consent mechanism can run, on a regulated financial platform where the user has not yet had any interaction with the app at all.

Fix: Remove directBootAware and gate Firebase initialization behind the app's own consent flow. No confirmation that this has occurred was ever received.

C2: Dual Biometric KYC Pipelines With No Documented DPIA Justification

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.

Fourthline (Netherlands) runs selfie liveness capture and NFC passport chip reading, both Art. 9(1) GDPR special-category biometric processing. A second, entirely separate KYC SDK, IDnow, is present in parallel in the same binary. Two independent biometric identity pipelines processing the same user, with no documented justification located for why both are necessary, is a DPIA gap on top of an already high-sensitivity processing activity.

```
com/fourthline/vision/selfie/ (selfie liveness capture)
com/fourthline/nfc/NfcAuthenticationChecks.smali (passport NFC chip)
de/idnow/sdk/ (parallel, second KYC pipeline, smali_classes4)
```

Impact: EU users undergoing KYC onboarding have their facial geometry and passport chip data processed by two separate biometric vendors with no documented reason the dual pipeline is necessary, and no disclosed retention period or sub-processor chain for either.

Fix: Document the specific necessity for running both Fourthline and IDnow in a DPIA, or consolidate to a single KYC pipeline. No confirmation that this has occurred was ever received.

C3: Braze Receives Trading Behavior and Location Data Linked to a Hardware Ad ID

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.

Braze Inc. (New York) is integrated with an active location module, receiving customer engagement data, including trading behavior, asset interests, and push notification interactions, linked to a hardware advertising ID. AD_ID and ACCESS_ADSERVICES_ATTRIBUTION permissions are both present alongside a duplicated ACCESS_COARSE_LOCATION declaration.

```
com/braze/location/ (active location module)
AD_ID, ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION
Braze Inc., 330 W 34th St, New York, NY 10001, USA
```

Impact: Financial behavioral data, a user's trading and asset-interest history, is transferred to US infrastructure and linked to a hardware advertising identifier, with an active location module present that raises the question of whether location and portfolio data are correlated on the vendor side.

Fix: Document the Art. 44 transfer mechanism covering Braze, and disable the location module unless a specific, disclosed feature requires it. No confirmation that this has occurred was ever received.

H1: Attribution SDK Links Advertising Campaigns to Trading Behavior

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.

The Adjust attribution SDK is present with signature-based attribution and the full set of AdServices attribution permissions. On a crypto trading platform, the in-app events Adjust ties to advertising campaigns are financial transactions and portfolio actions, a purpose materially different from providing a financial service.

Impact: A profile linking specific advertising campaigns to a user's actual trading behavior is created, a purpose that requires its own explicit consent, separate from the consent covering the financial service itself.

Fix: Obtain explicit, separate consent for attribution-linked trading-behavior profiling, or restrict Adjust to install-level attribution only. No confirmation that this has occurred was ever received.

H2: Datadog Session Monitoring Auto-Initializes and Transfers Data to the US

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.

Datadog Inc. (New York) is integrated via a ContentProvider that auto-initializes without explicit code invocation, running full real-user-monitoring: session capture, performance traces, UI interactions, and error events. On a platform handling financial transactions and KYC onboarding, session data may include sensitive user inputs.

```
DdRumContentProvider (auto-init ContentProvider)
Datadog Inc., 620 8th Avenue, New York, NY 10018, USA
```

Impact: Session-level UI interaction data from a regulated financial app, potentially including sensitive form inputs during KYC or transaction flows, reaches US infrastructure with no documented Art. 44 transfer mechanism.

Fix: Document the Art. 44 transfer mechanism covering Datadog, and exclude sensitive form fields from session capture. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 5(1)(a), Art. 5(1)(b), Art. 7	C1	Pre-consent tracking initialization on device boot, before consent.
Art. 9(1), Art. 9(2)(b), Art. 5(1)(b)	C2	Dual biometric KYC pipeline with no documented DPIA justification.
Art. 44, Art. 6(1)(a)	C3	Financial and location data transferred to US infrastructure, linked to a hardware ad ID.
Art. 6(1)(a), Art. 5(1)(b)	H1	Attribution SDK linking advertising campaigns to trading behavior.
Art. 44, Art. 5(1)(b)	H2	Auto-initializing US-bound session monitoring on a financial app.

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 CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own. In this report, C2 and C3 correct to HIGH on their own computed bands. C1, H1, and H2 correct to MEDIUM on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: BPND-2026-001.