Coordinated Security & Privacy Disclosure, Final Report

flatex Austria for Android (de.xcom.flatexat)

Eight written notices, ninety days, total silence – not even one automated acknowledgment

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FIVE FINDINGS UNADDRESSED AFTER EIGHT NOTICES, ZERO REPLIES OF ANY KIND

Target	flatexDEGIRO Bank AG, a BaFin/FMA-regulated bank serving approximately 3.5 million EU customers
Product audited	flatex Austria for Android, de.xcom.flatexat
Disclosure reference	REF FLATEXAT-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C1 hardcoded Firebase key enabling spoofed push notifications to all 3.5 million flatex customers, CVSS v4.0 8.8, 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 flatex Austria Android application, a licensed bank trading platform, and identified two CRITICAL and three HIGH findings: a Firebase API key hardcoded in the public APK capable of sending spoofed push notifications to the bank's entire customer base and reading Remote Config, both production and test Braze credentials present together in the shipped binary, with trading-behavior data flowing to a US marketing-automation vendor, a complete absence of any Network Security Configuration or certificate pinning on a licensed bank trading app, meaning login, portfolio queries, order placement, and account statements are protected only by Android's platform default trust store, an IDnow KYC biometric-verification integration processing live video, facial liveness detection, and ID document/NFC chip data with no documented Art. 35 DPIA or Art. 28(3) processing agreement visible, and the Braze integration itself as a separate data-flow concern under MiFID II Art. 25 suitability obligations given the trading-behavior categories it captures.

Across eight written notices over ninety days, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde, CERT.at, and the Hessian data protection authority, no reply of any kind was ever received, not a human response, not a ticket number, and not even an automated receipt confirmation, a case profile distinct from every other case in this disclosure wave, none of which produced total silence at every single one of eight attempts. None of RFI-IRFOS's five standing questions, on IDnow's Art. 9(2) legal basis and DPIA status, credential rotation, a certificate-pinning implementation timeline, the Art. 6(1)/MiFID II basis for the Braze transfer, or Art. 33 notification within 72 hours, ever received an answer.

Scope: Static analysis of the publicly downloaded production flatex Austria Android APK, on an authorized test device, only. No flatex account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@flatexdegiro.com, bcc the Austrian Datenschutzbehoerde, CERT.at, and the Hessian data protection authority (reflecting flatexDEGIRO Bank AG's Frankfurt/Hesse parent entity). Across eight written notices over ninety days, no reply of any kind was ever received, not a human response, not a ticket number, not even an automated receipt confirmation.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the public APK
C2	CRITICAL	Both production and test Braze credentials present in the production APK
H1	HIGH	No Network Security Configuration or certificate pinning on a licensed bank trading app
H2	HIGH	IDnow KYC biometric processing without a documented DPIA

ID	Severity	Title
H3	HIGH	Braze SDK: trading-behavior data flows into US marketing automation

Subject & Operator Analysis

flatexDEGIRO Bank AG is a BaFin/FMA-regulated bank headquartered in Frankfurt/Hesse, Germany, serving approximately 3.5 million EU customers through its flatex and DEGIRO trading brands. flatex Austria is its Austrian-market Android trading app.

Findings

C1: Firebase API key hardcoded in the public APK

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N, 8.8

A Firebase API key (AIzaSyA2Lxumh_lNKbQMdkjLNcnnm0tCQwIO_mI) is hardcoded in res/values/strings.xml, Firebase project flatex-at, database flatex-at.firebaseio.com . With it, spoofed push notifications can be sent to the bank's entire customer base, Remote Config can be read, and, depending on Firebase security rules, customer data or session information may be accessible.

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

Impact: A spoofed push-notification capability against a bank's entire customer base is a direct phishing and social-engineering vector, in addition to the standard risk a hardcoded Firebase key carries.

Fix: Rotate the exposed key, restrict it to the correct package name and SHA-256 signing fingerprint, and confirm deny-by-default Firebase security rules.

C2: Both production and test Braze credentials present in the production APK

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

Both braze_api_key and braze_api_key_test are present in the shipped binary, obfuscated but trivially reversible via standard reverse-engineering tooling. The test key ships to every one of 3.5 million flatex customers. The Braze endpoint (sdk.fra-01.braze.eu) correctly uses an EU cluster for data residency, but this does not remove the obligation to strip the credential entirely, and trading-behavior data still flows into a US-headquartered marketing-automation system.

No reply of any kind addressed this finding.

Impact: A test-environment credential shipped in a production banking app to millions of customers indicates a release-hygiene gap alongside the underlying data-transfer concern.

Fix: Remove both Braze credentials from the production build entirely and load them only via secure server-side configuration.

H1: No Network Security Configuration or certificate pinning on a licensed bank trading app

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

No android:networkSecurityConfig is declared in the manifest, and no Network Security Config file exists at all. All connections, login, portfolio queries, order placement, and account statements, are protected only by Android's platform-default trust store of roughly 150 system-trusted certificate authorities, with no SHA-256 pin for any flatex endpoint.

A realistic MITM scenario exists on corporate networks performing deep-packet inspection via an installed root certificate. No reply of any kind addressed this finding.

Impact: Login credentials, portfolio data, order instructions, and account statements on a licensed bank trading app can be intercepted or altered by any party able to install a trusted certificate on the network path.

Fix: Implement certificate pinning for all flatex endpoints.

H2: IDnow KYC biometric processing without a documented DPIA

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 IDnow SDK (IDnow GmbH, Munich, 1,433 smali classes) processes, during account opening, live video, facial liveness detection (biometric matching), ID document front and back, and NFC chip data for ePassport use. This is biometric data under Art. 4(14) and special-category data under Art. 9(1).

None of an Art. 28(3) processing agreement with IDnow, an Art. 35 DPIA, an explicit Art. 9(2) legal basis, or an Art. 13(1)(c) disclosure was visibly documented. No reply of any kind confirmed whether any of these exist.

Impact: Special-category biometric data collected during account opening may be processed without the documented legal basis and impact assessment Art. 9 and Art. 35 require.

Fix: Publish the Art. 28(3) processing agreement, Art. 35 DPIA, and Art. 9(2) legal basis covering IDnow's biometric verification.

H3: Braze SDK: trading-behavior data flows into US marketing automation

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

2,661 smali files implement the Braze SDK on a trading platform, likely capturing which instruments a customer views, login timestamps, market browsing, portfolio changes, order placement, and deposit/withdrawal triggers.

This touches MiFID II Art. 25 suitability and appropriateness obligations, in addition to the GDPR legal-basis question for transferring trading-behavior data to a marketing-automation vendor. No reply of any kind addressed this finding.

Impact: Detailed trading-behavior data may be processed for marketing-automation purposes with no confirmed Art. 6(1) legal basis specific to that use, on a platform separately subject to MiFID II suitability rules.

Fix: Confirm and publish the Art. 6(1) legal basis for trading-behavior data flowing to Braze, distinct from the basis for core trading-platform operation.

Eight Notices, Total Silence

This case is distinct from every other case in this disclosure wave: across eight written notices over ninety days, no reply of any kind was ever received from flatexDEGIRO, not a human response, not a ticket number, and not even a single automated receipt confirmation. RFI-IRFOS's own 18 August notice states this explicitly: 'fifty-eight days, four written notices to a BaFin- and FMA-regulated institution, not a single reply, not even an automated receipt confirmation.'

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1); EBA/GL/2019/04 Sec. 4.3	Hardcoded Firebase key enabling spoofed push notifications to the entire customer base
C2	GDPR Art. 32(1), Art. 28, Art. 44; EBA/GL/2019/04 Sec. 4.3	Production and test credentials both shipped, trading data to a US vendor
H1	GDPR Art. 32(1)(a), Art. 25; EBA/GL/2019/04 Sec. 4.4	No certificate pinning on any bank trading endpoint
H2	GDPR Art. 9, Art. 13(1)(c), Art. 28(3), Art. 35	Undocumented DPIA and legal basis for biometric KYC processing
H3	GDPR Art. 5(1)(c), Art. 6(1), Art. 13(1)(e); MiFID II Art. 25	Trading-behavior data transferred to a marketing-automation vendor

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@flatexdegiro.com, bcc Austrian DSB/CERT.at/Hessian DPA; 2 CRITICAL + 3 HIGH findings; a EUR 75,000 NDA research-engagement figure was referenced under the R1 policy then in force – historical record only, not a currently open offer
2026-06-28	Follow-up #1, seven days, no response, response deadline of 2 July set
2026-08-18	Follow-up #4, day 58, four written notices, not even an automated acknowledgment, deadline of 25 August set for certificate pinning and the Art. 9 question
2026-09-03	Follow-up #5, day 74, 25 August deadline elapsed
2026-09-16	Follow-up #7, seven notices since 21 June, zero reactions, weekly SHA-256 re-hashing during the embargo disclosed, embargo confirmed 3 days away
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Establish a functioning response process for GDPR disclosures sent to a regulated institution's own datenschutz@ mailbox.
- Implement certificate pinning across all flatex trading, login, and account-statement endpoints.
- Publish the Art. 35 DPIA and Art. 28(3) processing agreement covering IDnow's biometric KYC processing.
- Rotate the exposed Firebase key and remove both Braze credentials from the production build.
- Confirm the Art. 6(1) legal basis for trading-behavior data flowing to Braze, separate from core platform operation.

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. 5, 6, 9, 13, 25, 28, 32, 35, 44. EBA/GL/2019/04. MiFID II Art. 25. REF FLATEXAT-2026-R1.