Coordinated Security & Privacy Disclosure, Final Report

George for Android (at.erstebank.george)

Five days of real technical dialogue, one disputed fix, and two findings, undisclosed behavioral biometrics and undisclosed US-routed banking calls, that never received a single word of response across ninety days

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – C1/H1/H4 DISPUTED, H2/H3 NEVER ANSWERED AT ALL

Target	Erste Bank der oesterreichischen Sparkassen AG / Erste Digital GmbH, Vienna, Austria
Product audited	George for Android, at.erstebank.george, v26.14.24
Disclosure reference	REF GEORGE-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (H2 ThreatFabric behavioral biometrics / H3 Azure-Teams call routing, CVSS v4.0 8.7, never answered at all)

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 George Android banking application, covering Austria and six other markets, and identified one CRITICAL and eight HIGH findings across two rounds: an inconsistent TLS certificate-pinning configuration where Austrian production banking traffic is protected only by system-CA trust while the equivalent Czech traffic is properly pinned; undisclosed Art. 9 biometric processing during KYC onboarding (Innovatrics IDKit); an undisclosed behavioral-biometric SDK (ThreatFabric) uploading keystroke dynamics and device fingerprints off-device; undisclosed US-routed banking support calls via Microsoft Azure Communication Services and Teams; continuous background location tracking on a banking app; and a second round of four findings, Google Analytics 4, hardcoded Firebase keys, the Adjust attribution SDK, and Datadog session-replay monitoring, all active in production banking infrastructure.

Balázs György of Erste Digital's Critical Incident Response Center engaged substantively across five days. On the certificate-pinning finding, Erste stated the specific domain found was an internal testing artifact that does not resolve externally, and would be removed from the Czech configuration rather than added to Austria's; RFI-IRFOS's position is that this confirms rather than eliminates the underlying gap, since it does not establish what Austria's actual production banking hostnames are or whether they are pinned to the same standard as the Czech market. On the biometric and location findings, Erste stated consent is collected and can be revoked, without demonstrating the actual consent flow when directly asked to. On the four second-round findings, Erste stated it had not found evidence of three of them in the Austrian build and requested more context, which RFI-IRFOS declined to supply beyond what a formal paid engagement would cover.

After 26 June 2026, Erste never replied again, across ten written notices and eighty-five days. Two findings, an undisclosed behavioral-biometric SDK uploading data to Amsterdam, and undisclosed US-routed banking support calls via Microsoft's infrastructure with no documented Art. 46 transfer mechanism, never received a single word of response, not agreement, not denial, not a request for detail, at any point across the entire case.

Scope: Static analysis of the publicly downloaded production George Android APK (v26.14.24), on an authorized test device, only. No George account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@erstebank.at, cc security@erstebank.at, bcc the Austrian DSB and CERT.at. Balázs György of Erste Digital's Critical Incident Response Center engaged substantively across five days, disputing several findings and disclosing a partial fix for one. From 26 June 2026 onward, across ten written notices and eighty-five days, Erste never replied again. Two HIGH findings, undisclosed behavioral-biometric collection and undisclosed US-routed banking support calls, never received a single word of response at any point in the case.

ID	Severity	Title
C1	CRITICAL	Certificate-pinning gap: Austrian production banking traffic unpinned where Czech production is correctly pinned
R1-H1	HIGH	Innovatrics IDKit biometric KYC processing, consent flow never demonstrated
R1-H2	HIGH	ThreatFabric behavioral-biometric SDK, undisclosed off-device upload, never answered
R1-H3	HIGH	Azure Communication Services and Microsoft Teams route banking support calls, no documented Art. 46 transfer mechanism, never answered
R1-H4	HIGH	Continuous background location tracking on a banking app, consent flow never demonstrated
R2-H1	HIGH	Google Analytics 4 active in a banking app
R2-H2	HIGH	Hardcoded Firebase API keys and project identifiers in a bank's production APK
R2-H3	HIGH	Adjust attribution SDK active in banking infrastructure
R2-H4	HIGH	Datadog RUM session-replay capability active in a banking context

Subject & Operator Analysis

George is Erste Group's digital banking platform, covering Austria, Czechia, Slovakia, Hungary, Croatia, Serbia, and Romania. This case concerns the Austrian market build; Erste Digital GmbH's Critical Incident Response Center in Vienna handled the correspondence.

Positive Observations

- Erste's Critical Incident Response Center engaged quickly and substantively across the first five days, a genuinely rare response speed in this research series.
- Erste correctly identified and disclosed that the specific pinning-gap domain RFI-IRFOS cited was an internal testing artifact, independently confirmed by RFI-IRFOS via NSLOOKUP, rather than disputing it outright.

Findings

C1: Certificate-pinning gap: Austrian production banking traffic unpinned where Czech production is correctly pinned

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

Czech production's network security config pins georgebffcz.erste-group.net and csas.cz with custom CA pins. Austrian production's equivalent config pins only a blog domain, a Luxembourg entity domain, and sparkasse.at, with erste-group.net absent entirely; Austrian banking traffic falls back to system-CA trust alone.

Erste's 26 June reply stated the specific domain RFI-IRFOS found was an internal testing artifact, verified by RFI-IRFOS via NSLOOKUP to return NXDOMAIN, and would be removed from the Czech configuration rather than added to Austria's, stating "for us this eliminates the finding." RFI-IRFOS's position, stated the same day: a phantom pinning entry existing and being silently corrected confirms the underlying inconsistency rather than resolving it, and does not establish what Austria's real production BFF hostnames are or whether they are pinned to the Czech standard. This question was repeated in every subsequent follow-up and never answered.

Impact: Austrian banking API traffic is protected only by system-CA trust, meaning any actor holding a system-trusted certificate, enterprise MDM, a rogue access point, or a compromised CA, can intercept identical financial transaction data that the Czech market protects with certificate pinning.

Fix: Publish the actual Austrian production BFF hostnames and confirm they carry the same certificate pinning as the Czech market equivalent.

R1-H1: Innovatrics IDKit biometric KYC processing, consent flow never demonstrated

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

88 smali files implement facial liveness detection and NFC biometric passport chip reads (ICAO LDS DG13/DG2 data), both Art. 9(1) special-category biometric data, during onboarding KYC.

Erste's reply: "used during onboarding for KYC after consent." RFI-IRFOS's rebuttal asked Erste to show where and how granular, separate Art. 9(2)(a) consent, distinct from general terms and conditions, is actually collected before processing begins. No consent-flow evidence was ever provided.

Impact: Special-category biometric processing occurs without demonstrated evidence of the granular consent GDPR Art. 9(2)(a) requires.

Fix: Publish the actual onboarding screen sequence showing where separate, explicit biometric consent is captured.

R1-H2: ThreatFabric behavioral-biometric SDK, undisclosed off-device upload, never answered

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

23 smali files implement a local behavioral-biometric database (keystroke dynamics, swipe velocity and pressure, interaction timing) and a device-fingerprint database, with a confirmed upload worker sending this data off-device to ThreatFabric's servers in Amsterdam.

This finding received zero response from Erste at any point across the entire case, not agreement, not denial, not a request for more detail, from the first notice on 21 June through the final follow-up on 4 September.

Impact: Behavioral biometric data, constituting GDPR Art. 4(14) biometric data, is collected and transmitted to an undisclosed sub-processor with no confirmed Art. 13(1)(e) disclosure.

Fix: Name ThreatFabric explicitly as a processor in George's Art. 13 privacy notice, and document the Art. 6 legal basis for this collection.

R1-H3: Azure Communication Services and Microsoft Teams route banking support calls, no documented Art. 46 transfer mechanism, never answered

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

Named classes confirm banking support agents join customer calls via Microsoft Teams, with Azure Communication Services routing call audio and video, and a screen-capture foreground service enabling screen sharing of banking data during calls, with no explicit EU data-residency configuration found in the binary.

Microsoft is not named as a call-data processor in George's published Art. 13 privacy notice per RFI-IRFOS's review. Like R1-H2, this finding received zero response from Erste at any point in the correspondence.

Impact: Banking support call data may transit US Azure infrastructure with no documented Art. 46 transfer safeguard on file.

Fix: Confirm EU data-residency configuration for Azure Communication Services, name Microsoft as a processor, and publish the applicable Art. 46 transfer mechanism.

R1-H4: Continuous background location tracking on a banking app, consent flow never demonstrated

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

ACCESS_BACKGROUND_LOCATION is used by TravelHub's geofencing components to detect international border crossings, allowing continuous location updates even when the app is not in use, on an app holding full transaction history, IBAN data, and investment portfolios.

Erste's reply: "used to provide relevant information right after border crossing. It can be revoked at any time." RFI-IRFOS's rebuttal: revocability after the fact does not satisfy Art. 6(1)(a)'s requirement for informed, granular consent collected before processing begins. The actual consent flow was never shown.

Impact: Combined with full financial data, continuous background location creates a high-granularity movement profile without demonstrated pre-processing consent.

Fix: Publish the actual consent screen shown before TravelHub begins background location tracking.

R2-H1: Google Analytics 4 active in a banking 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, 6.9

GA4 SDK present and active in the production APK, transmitting financial navigation events to Google.

Erste's reply: "We have not found evidence of using these in George AT, more context is needed." RFI-IRFOS declined to supply further smali-level technical depth outside a formal paid engagement, leaving the finding as an unresolved standoff on the binary evidence RFI-IRFOS holds.

Impact: Financial navigation behavior is potentially exposed to Google without a resolved dispute over whether the SDK is actually active.

Fix: Confirm GA4's activation status in the Austrian build directly against the binary, rather than by internal search alone.

R2-H2: Hardcoded Firebase API keys and project identifiers in a bank's 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

Firebase API keys and project identifiers hardcoded in the production APK.

Erste's defense cited Google's own documentation that Firebase keys are "public by design." RFI-IRFOS's rebuttal named three concrete attack vectors this framing does not address: quota-exhaustion denial of service requiring no authorization, exploitation of any misconfigured Firebase Security Rule using the key as the only credential, and enumeration of Remote Config feature flags, kill switches, and portal endpoints if not explicitly restricted.

Impact: A public-by-design credential still exposes concrete denial-of-service and misconfiguration risk specific to this Firebase project.

Fix: Confirm Firebase Security Rules are deny-by-default and Remote Config access is restricted, and publish that confirmation.

R2-H3: Adjust attribution SDK active in banking infrastructure

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 mobile-attribution and advertising SDK is present and active in the production banking APK.

Erste's reply: "We have not found evidence of using these in George AT, more context is needed." Left as an unresolved standoff, same as R2-H1.

Impact: An advertising-attribution SDK's presence in banking infrastructure remains disputed rather than confirmed or ruled out.

Fix: Confirm Adjust's activation status in the Austrian build directly against the binary.

R2-H4: Datadog RUM session-replay capability active in a banking context

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

Datadog Real User Monitoring is present and active, with session-replay capability capable of recording financial-interaction sessions.

Erste's reply: "We have not found evidence of using these in George AT, more context is needed." Left as an unresolved standoff, same as R2-H1 and R2-H3.

Impact: Session-replay capability on a banking interface, if active, would capture visual financial data with no resolved confirmation either way.

Fix: Confirm Datadog RUM's activation and session-replay status in the Austrian build directly against the binary.

Five Days of Real Dialogue, Then Eighty-Five Days of Silence

Balázs György's four replies between 22 and 26 June 2026 addressed most findings directly, disputing several and disclosing a partial fix for the pinning gap. After 26 June, across ten written notices, including a formal Art. 33(4) notice, an escalation to Erste Group's Chief Platform Officer, and a full-chronology recap, Erste did not reply again at all. Two of the nine findings, R1-H2 and R1-H3, never received any response whatsoever at any point in the case, a fact RFI-IRFOS stated explicitly in its own 4 September follow-up: "has never received a single word of response, not agreement, not denial, not a request for more detail."

Finding	Provision	Concern

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25, Art. 32(1)(a)	Inconsistent TLS pinning across markets processing identical financial data
R1-H1	GDPR Art. 9(1), Art. 9(2)(a)	Biometric KYC processing, consent flow undemonstrated
R1-H2	GDPR Art. 4(14), Art. 13(1)(e)	Undisclosed behavioral-biometric sub-processor
R1-H3	GDPR Art. 13(1)(e), Art. 46	Undisclosed US-routed call data, no transfer mechanism on file
R1-H4	GDPR Art. 5(1)(c), Art. 6(1)(a)	Continuous background location, consent flow undemonstrated
R2-H1/H3/H4	GDPR Art. 13(1)(e)	Disputed SDK activation status, unresolved stand-off
R2-H2	GDPR Art. 32	Hardcoded credential, DoS and misconfiguration exposure

Date	Event
2026-06-26	Erste's most substantive reply: partial pinning-gap fix disclosed, other findings disputed or unconfirmed; last real reply of the case
2026-07-05 through 2026-08-24	Five follow-ups repeat the same three unanswered questions; Chief Platform Officer added to the thread; Art. 33(4) formally invoked
2026-09-04	Final follow-up states explicitly that R1-H2 and R1-H3 never received any response at all
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Publish the actual Austrian production BFF hostnames and confirm certificate pinning matches the Czech market standard.
- Answer R1-H2 (ThreatFabric) and R1-H3 (Azure/Teams) on the merits, given they have received no response of any kind in ninety days.
- Demonstrate the actual consent-collection screens for Art. 9 biometric processing and background-location tracking.

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