Coordinated Security & Privacy Disclosure, Final Report

Bolt for Android (ee.mtakso.client)

A closed loop: privacy points to security, security answers with a bug-bounty bot, ninety days, no named contact ever

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, A CLOSED DEFLECTION LOOP, NO NAMED CONTACT EVER

Target	Bolt Technology OU, Tallinn, Estonia
Product audited	Bolt for Android, ee.mtakso.client, build CA.214.0
Disclosure reference	REF BOLT-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 hardcoded Firebase keys, CVSS v4.0 9.3)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Bolt Android application and identified six findings, two CRITICAL, four HIGH. The most significant: three hardcoded Firebase production API keys remain in the shipped APK, pointed at a database still named taxify-client, the brand Bolt retired in its 2019 rebrand, indicating these exact credentials have shipped unrotated for at least seven years, the longest-standing hardcoded credential exposure identified across this year's research series.

Separately, an advertised migration from Google Maps to Mapbox, intended to reduce Google location telemetry, has not shipped, Google Maps SDKs remain active with no Mapbox SDK present, and certificate pinning could not be verified as active anywhere in the binary despite the app transmitting real-time location, payment, and biometric data. Four further findings raise separate concerns: calendar access co-present with a marketing SDK with no disclosed data boundary; continuous background location tracking outside active rides; Veriff facial-biometric and NFC passport-chip KYC processing with no confirmed DPIA; and Vulog BLE vehicle-unlock infrastructure operating as an undisclosed third-party processor.

Twelve written notices were sent over 90 days. security@bolt.eu answered every one with an identical Bugcrowd bug-bounty autoresponder. privacy@bolt.eu sent several near-identical templated replies redirecting back to security@bolt.eu, closing the loop. Three specific named questions, on credential rotation, pinning verification, and a named contact, were asked repeatedly and never answered by anyone with a stated role.

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

Disposition

R1 sent 20 June 2026 to security@bolt.eu, bcc the Austrian DSB, CERT.at, and Estonia's Andmekaitse Inspektsioon. Twelve written notices followed. security@bolt.eu answered every single one with an identical Bugcrowd bug-bounty autoresponder; privacy@bolt.eu answered with templated redirects back to security@bolt.eu. Not one message in the entire correspondence came from a named individual with a stated role who engaged with any finding on its technical merits.

ID	Severity	Title
C1	CRITICAL	Three hardcoded Firebase production keys, still branded taxify-client, at least seven years unrotated
C2	CRITICAL	Advertised Maps-to-Mapbox migration not shipped, certificate pinning unverifiable
H1	HIGH	Calendar access co-present with a marketing SDK, no disclosed data boundary
H2	HIGH	Continuous background location tracking outside active rides

ID	Severity	Title
H3	HIGH	Veriff SDK: facial biometrics and NFC passport-chip KYC, no confirmed DPIA
H4	HIGH	Vulog BLE vehicle-unlock SDK: undisclosed third-party processor

Subject & Operator Analysis

Bolt Technology OU (Tallinn, Estonia) operates the Bolt ride-hailing platform, with Estonia's Andmekaitse Inspektsioon as lead GDPR supervisory authority.

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: Three hardcoded Firebase production keys, still branded taxify-client, at least seven years unrotated

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

Three Firebase credentials are hardcoded in the shipped APK. The database URL, taxify-client.firebaseio.com, references the Taxify brand retired in Bolt's 2019 rebrand.

```
AIzaSyBCrsKCcwYojdbT_ALZ9qI8hl2Z_pnZQw8
AIzaSyCEcs8rW-83laJLGF-oSUTPFvnv1dJi47E
AIzaSyCpRzs_1Aiz8KOQiXFKU-2Ksh2U1zKqpPI
Database: https://taxify-client.firebaseio.com
```

No response was received naming this finding, including three separate requests for confirmation that these keys have been rotated or restricted to package plus SHA-256 fingerprint. The taxify-client naming indicates continuous unrotated use for at least seven years, the longest-standing hardcoded credential exposure identified across this year's research series.

Impact: Three publicly extractable credentials, unrotated for at least seven years, enable probing of the Firebase project and potential further backend access.

Fix: Rotate all three credentials, restrict them to the production certificate fingerprint, and confirm the rotation in writing.

C2: Advertised Maps-to-Mapbox migration not shipped, certificate pinning unverifiable

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

Google Maps SDKs remain active in the shipped binary; no Mapbox SDK or access token was found, meaning an advertised migration intended to reduce Google location telemetry has not shipped. No network security configuration with domain entries was found, and while OkHttp's CertificatePinner class is referenced, no pin hash values could be identified.

No response was received naming this finding, including the direct request to verify pinning status. For an app transmitting real-time location, payment, and biometric data, certificate pinning must be verifiably active; it currently cannot be confirmed as such from the binary.

Impact: Real-time location, payment, and biometric data traffic has no confirmed certificate-pinning protection, and a location-telemetry-reduction migration announced to users has not actually shipped.

Fix: Complete the Mapbox migration or disclose that Google location telemetry continues, and publish verifiable certificate-pinning configuration for all production API endpoints.

H1: Calendar access co-present with a marketing SDK, no disclosed data boundary

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

A CalendarSuggestions feature reads calendar events, appointment titles, meeting locations, and schedules, to suggest pre-booked rides, co-present with the Braze marketing SDK (934 classes).

No response was received naming this finding. Whether calendar data feeds Braze targeting is not determinable from static analysis alone, but the co-presence of calendar access and a marketing SDK requires explicit disclosure of the data boundary between them, which was not found in Bolt's privacy policy.

Impact: Calendar data, including appointment titles and meeting locations, is accessed with no disclosed boundary against a co-present marketing SDK.

Fix: Disclose whether calendar data is shared with or accessible to the Braze marketing SDK, and publish the specific purpose limitation under Art. 5(1)(b).

H2: Continuous background location tracking outside active rides

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

ACCESS_BACKGROUND_LOCATION enables continuous tracking while the app is backgrounded and no ride is active.

No response was received naming this finding. This is not necessary for delivering the transportation service and enables persistent daily movement profiling beyond Bolt journeys themselves.

Impact: Users' daily movement patterns may be profiled continuously, independent of and beyond any active ride.

Fix: Restrict location collection to periods when a ride is active or being requested, per Art. 5(1)(c) data minimization.

H3: Veriff SDK: facial biometrics and NFC passport-chip KYC, no confirmed 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

652 combined Veriff classes process facial liveness biometrics and NFC chip-level passport data for driver KYC verification.

No response was received naming this finding. This is Art. 9(1) special-category biometric data, and the Art. 36 DPIA consultation obligation applies to this processing stack; no confirmation of a completed DPIA was received.

Impact: Special-category biometric and passport data is processed for driver verification with no confirmed Art. 36 DPIA.

Fix: Confirm and publish the Art. 36 DPIA covering the Veriff KYC processing stack.

H4: Vulog BLE vehicle-unlock SDK: undisclosed third-party processor

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

121 Vulog (France) classes send BLE commands to physically unlock Bolt vehicles, receiving vehicle ID, unlock time, duration, and location as a data processor.

No response was received naming this finding. Vulog is not listed in Bolt's privacy notice as a data processor.

Impact: Vehicle-session data including precise unlock location and duration is processed by an undisclosed third-party processor.

Fix: Name Vulog as a data processor under Art. 13(1)(e) and publish the applicable data-processing agreement scope.

Bolt's Response, Recorded in Full: A Closed Deflection Loop

Every one of RFI-IRFOS's twelve written notices to security@bolt.eu received the identical automated reply: "You can submit any vulnerability finding in our system and product to our bounty program on Bugcrowd at https://bugcrowd.com/engagements/bolt-og. In case of personal data related questions please contact us at: https://bolt.eu/en/privacy/."

privacy@bolt.eu replied several times with near-identical templates redirecting the disclosure back to security@bolt.eu, closing the loop. "Selina, Bolt Team" wrote on 29 June: "Please check the guidelines for responsible disclosure... Please email security@bolt.eu if you believe your report aligns with the guidelines." A reply signed "Bolt Customer Support" on 6 August named the specific GDPR articles at issue, "your formal disclosure and questions regarding GDPR compliance (Art. 6, 28) and internal credential management," but nonetheless redirected again: "need to be escalated directly to the email address stated previously security@bolt.eu."

RFI-IRFOS's own 18 August letter documents this pattern directly: "Not one message in this entire chain has come from a named individual with a stated role, and not one has addressed a single finding." Three specific questions, the name and role of a responsible contact, the rotation status of the three Firebase keys, and confirmation that certificate pinning is verifiably active, were asked repeatedly through the final message on 4 September and never answered by anyone able or willing to give a substantive answer.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b)	Hardcoded, unrotated credentials, at least seven years old
C2	GDPR Art. 32(1)(a)	Unverifiable certificate pinning, incomplete location-SDK migration
H1	GDPR Art. 5(1)(b), Art. 13, Art. 6	Undisclosed data boundary between calendar access and marketing SDK
H2	GDPR Art. 5(1)(c)	Continuous background location tracking outside active use
H3	GDPR Art. 9(1), Art. 36	Biometric and passport KYC data, no confirmed DPIA
H4	GDPR Art. 5(1)(c), Art. 13(1)(e)	Undisclosed third-party vehicle-unlock processor

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to security@bolt.eu, bcc Austrian DSB/CERT.at/Estonian AKI, 6 findings; Bugcrowd autoresponder received same day
2026-06-28 / 06-29	Follow-ups to privacy@bolt.eu; "Selina, Bolt Team" redirects to security@bolt.eu twice
2026-07-24	Follow-up, EDPS added to cc; privacy@bolt.eu sends processing acknowledgment then repeats the guidelines-redirect template
2026-08-05 / 08-06	Follow-ups; privacy@bolt.eu repeats the redirect template three more times, one instance naming GDPR Art. 6/28 by name but still redirecting
2026-08-18	Full documented chronology of the closed deflection loop sent, regulators moved from bcc to visible cc, deadline set 25 August
2026-08-28	25 August deadline passed unanswered; full findings restated, three named questions posed again, new deadline 4 September
2026-09-04	Final follow-up restates C1/C2 with full technical detail; only reply is the identical Bugcrowd autoresponder
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Twelve written notices across 90 days produced a closed deflection loop between an automated security bot and a templated privacy-team redirect. Not one message in the entire correspondence came from a named individual with a stated role who engaged with any of the six findings on their technical merits.

Residual Risk & Recommendations

- Rotate all three Firebase credentials and confirm the rotation in writing; this is the single highest-priority item given at least seven years of continuous exposure.
- Publish verifiable certificate-pinning configuration for all production endpoints handling location, payment, and biometric data.
- Confirm and publish the Art. 36 DPIA covering the Veriff biometric and passport KYC processing stack.
- Name Vulog as a data processor and restrict background location collection to active-ride periods.
- Establish a named, reachable contact for security and privacy disclosures independent of the Bugcrowd bounty portal and the closed privacy/security redirect loop documented in this report.

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. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 9, 13, 28, 32, 36. REF BOLT-2026-R1.