Coordinated Privacy Disclosure, Final Report

MySantander Android (de.santander.presentation)

Santander Consumer Bank AG, Mönchengladbach, Germany

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE STATED 19 SEPTEMBER EMBARGO, EIGHT MESSAGES, ZERO REPLY OF ANY KIND

Target	MySantander, the customer banking app for Santander Consumer Bank AG
Package	de.santander.presentation, version 2.81.0
Operator	Santander Consumer Bank AG, Mönchengladbach, Germany
Initial Disclosure	2026-06-25
Stated Embargo	2026-09-19, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, six days after the stated date
Regulators	LDI NRW (lead SA), BSI CERT-Bund, Austrian DSB, CERT.at, EDPS
Total Outbound Messages	8, across 51 days, all to datenschutz@santander.de.
Inbound Replies	0. No reply, automated or human, 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 25 June 2026, RFI-IRFOS disclosed to Santander Consumer Bank AG that its MySantander Android app is, by the standard of this audit campaign, a genuinely careful build, and structured the disclosure to lead with that assessment before the three findings. The app implements certificate pinning on its primary secure endpoint, its custom trust managers validate correctly, not accepting all certificates, it ships no advertising-ID permission, no location access, and no microphone access, and it targets a current Android SDK. Several banks reviewed in this campaign do none of these things.

Against that baseline, three findings remain. The Adjust SDK performs install attribution and device-signal collection on a regulated banking app; RFI-IRFOS noted explicitly that Santander did not declare the AD_ID permission, meaning the advertising identifier returns zeros on Android 13 and later, a deliberate and privacy-conscious choice that narrows the finding to a single open question: the specific Art. 6(1)/7 lawful basis for Adjust's remaining data collection, and where it is disclosed under Art. 13. Dynatrace was assessed as legitimate first-party operational monitoring and flagged only for completeness, not as a finding in its own right.

A second finding names a hardcoded, extractable Firebase API key, standard boilerplate in this campaign's findings but still worth confirming is properly restricted for a bank. A third finding is explicitly framed as a resilience gap, not a security hole: certificate pinning on the app's primary endpoint appears to use a single pin with no published backup, meaning a routine certificate rotation without a pre-shipped backup pin could hard-fail pinning for live users; a second API host referenced in the code was not statically confirmed as either pinned or unpinned, and the disclosure was explicit that it was not asserting the second host was unprotected.

Eight messages were sent across 51 days, all to datenschutz@santander.de, cc'ing LDI NRW (the lead supervisory authority for Santander's Mönchengladbach establishment), BSI CERT-Bund, the Austrian DSB, CERT.at, and the EDPS throughout. Not one reply, automated or human, was ever received, even a brief acknowledgment of an unusually positive report. The 90-day embargo, stated directly to the target in the initial disclosure, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production MySantander Android application (de.santander.presentation, version 2.81.0, SHA-256 27f715c033145a3e7f0374f41359c756e65c79c08ef2ea922d52342e8fd86dd6), pulled from Google Play and reviewed on 25 June 2026. No account was created and no interaction with Adjust's, Dynatrace's, or Firebase's backend infrastructure was performed.

Disposition

Three findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. All three correct to MEDIUM on their own computed bands: an unresolved lawful-basis question for the Adjust marketing-attribution SDK on a banking app, an extractable Firebase API key, and single-pin certificate pinning with no backup pin. This is among the cleanest builds reviewed in this campaign, and the disclosure led with that assessment. Eight messages were sent across 51 days. Not one reply of any kind was ever received, even to acknowledge an unusually positive report.

ID	Severity	Title
F1	MEDIUM	Marketing-Attribution SDK's Lawful Basis Unconfirmed on a Regulated Bank
F2	MEDIUM	Extractable Firebase API Key
F3	MEDIUM	Single Certificate Pin With No Backup Pin

Subject & Operator Analysis

Santander Consumer Bank AG is established in Mönchengladbach, Germany, placing LDI NRW (Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen) as lead supervisory authority, with BSI CERT-Bund as the relevant national CSIRT. Santander Consumer Bank also operates in Austria, so the Austrian DSB and CERT.at were copied as well.

Genuine positives are extensive here and are worth stating plainly. Certificate pinning is implemented on the app's primary secure endpoint. Custom trust managers validate correctly, not accepting all certificates. The permission set is clean and proportionate: no advertising-ID permission, no location access, no microphone access. The app targets a current Android SDK (36), and pre-consent tracking surface is minimal. Several banks reviewed in this campaign implement none of these protections.

Eight Messages, Zero Reply

All eight messages in this case's correspondence record were delivered to datenschutz@santander.de across 51 days, cc'ing LDI NRW, BSI CERT-Bund, the Austrian DSB, CERT.at, and the EDPS throughout. Not one reply, automated or human, was ever received on that address at any point, notably including no acknowledgment of what was, for this campaign, an unusually favorable assessment.

Findings

F1: Marketing-Attribution SDK's Lawful Basis Unconfirmed on a Regulated Bank

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 SDK and AdvertisingIdClient are present, alongside Dynatrace RUM and Firebase. The AD_ID permission is not declared, meaning the advertising identifier correctly returns zeros on Android 13 and later, a deliberate and privacy-conscious mitigation. Adjust still performs install attribution and device-signal collection, and the specific Art. 6(1)/7 lawful basis, and its disclosure under Art. 13, was not confirmed.

```
Adjust SDK + AdvertisingIdClient present (AD_ID permission not declared)
Dynatrace RUM assessed as legitimate first-party operational monitoring
```

Impact: A marketing-attribution platform on a regulated banking app requires a documented lawful basis distinct from the app's own operational purpose, and that basis was not visible from the outside despite the app's otherwise privacy-conscious configuration.

Fix: State the specific Art. 6(1)/7 basis for Adjust and confirm its disclosure in the privacy policy under Art. 13. No confirmation that this has occurred was ever received.

F2: Extractable Firebase API Key

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.

A Firebase API key is hardcoded and extractable from the production binary.

```
google_api_key: AIzaSyCd19XIyT_oon0CLogDHDloJTYlBJqL7Fg
```

Impact: An extractable key can be driven until quota is exhausted, a customer-facing denial-of-service risk, and grants access if security rules are not deny-by-default; for a bank the expectation is that restriction and App Check are already in place, but this was not independently confirmable.

Fix: Confirm key restriction by package and certificate, App Check enforcement, and deny-by-default security rules. No confirmation that this has occurred was ever received.

F3: Single Certificate Pin With No Backup Pin

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3.

The certificate pin on secure.meine.santander.de appears to be a single pin with no published backup pin. A second API host referenced in the code, api2.santander.de, was not statically confirmed as either pinned or unpinned; this finding does not assert that host is unprotected.

Impact: This is explicitly a resilience gap, not a confirmed security hole: a routine certificate rotation without a pre-shipped backup pin can hard-fail pinning for live users, a self-inflicted availability problem, not an exploitable weakness.

Fix: Add at least one backup pin per Android's own guidance, and confirm pin coverage across all banking API hosts including api2.santander.de. 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. 6(1), Art. 7, Art. 13	F1	Unconfirmed lawful basis for a marketing-attribution SDK.
Art. 32	F2	Extractable Firebase API key.
Art. 32 (resilience)	F3	Single certificate pin with no backup.

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, all three findings correct to MEDIUM on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: SANTANDER-R1.