



Security & Privacy Disclosure, Final Report

SPAR Plus (plus.spar.si), production APK, 48.2 MB, 39,424 smali classes, analyzed 2026-06-30

A hardcoded SAP Gigya identity-infrastructure key sits alongside two Firebase keys, a Maps key and an exposed production database, an Emarsys geofence receiver that registers location-based marketing zones at system boot before the app is ever opened, and a contacts-reading task in SPAR's own code, unresolved through 109 days and nine messages, 19 days past an unmoved embargo, with zero reply of any kind ever received from SPAR

PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28 SEPTEMBER 2026, ALL FIVE FINDINGS REMAIN UNADDRESSED

Target	SPAR d.o.o., Ljubljana, Slovenia (SPAR Slovenia; parent: SPAR International Holding, Salzburg, Austria)
Package	plus.spar.si
Version Audited	Production APK, Google Play, analyzed 2026-06-30 (48.2 MB, 39,424 smali classes)
Platform	Android, static analysis
Initial Disclosure (R1)	2026-06-30 (REF PLUS.SPAR.SI)
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	5 (2 Critical, 3 High)
Correspondence	9 messages sent by RFI-IRFOS over 109 days (30 June through 12 September 2026) to security@spar.si, zasebnost@spar.si, odnosi-z-javnostmi@spar.si, and dpo@spar.si; zasebnost@spar.si, odnosi-z-javnostmi@spar.si, and dpo@spar.si all hard-bounced (address unknown) on every attempt; security@spar.si accepted every message without a single bounce and never once replied
Authorities CC'd / BCC'd	Informacijski pooblaščenec (IP), Ljubljana — lead supervisory authority for SPAR d.o.o.; Austrian Datenschutzbehörde (DSB) and CERT.at from the research institute's own jurisdiction; European Data Protection Supervisor (EDPS) for the Salzburg-based parent group

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1	Executive Summary	4
2	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	6
4.1	C1: Two Firebase keys, a Google Maps key, and the production database URL hardcoded in the distributed binary	6
4.2	C2: SAP Gigya (CIAM) API key hardcoded: identity, login, and consent-management infrastructure exposed	7
4.3	H1: Emarsys geofence registration at system boot: location-based marketing before the app is opened and before any consent	8
4.4	H2: ReadPhoneContactsTask in SPAR's own code: third-party contact data read for a shopping-list-sharing feature	8
4.5	H3: Firebase pre-consent initialization plus Android Privacy Sandbox attribution and advertising-ID permissions	9
5	Impact Analysis	9
6	The Complete Chain: Nine Messages Across 109 Days, Zero Replies Of Any Kind	10
7	Disclosure Timeline & Outcome	11
8	Data Protection — Article by Article	11
9	Regulatory Landscape & Fine Exposure	12
10	Indicators of Compromise	12
11	Residual Risk & Recommendations	12

Executive Summary

SPAR d.o.o., the Slovenian operating entity of the SPAR International retail group (headquartered in Salzburg, Austria), operates the SPAR Plus loyalty and shopping app for the Slovenian market. A static analysis of the production Android APK (plus.spar.si), performed 2026-06-30, identified five findings, two CRITICAL and three HIGH, spanning credential hardcoding across two separate platforms, pre-consent location tracking, and undisclosed contacts access.

Two Firebase API keys, a Google Maps API key, and the production Firebase Realtime Database URL are hardcoded in res/values/strings.xml (C1), present verbatim in every installed copy and exploitable for quota exhaustion or, if security rules are misconfigured, direct database access. Separately, and more severely, the SAP Gigya Customer Identity and Access Management (CIAM) API key is also hardcoded (C2): Gigya is the identity and consent-management platform behind the entire SPAR customer account system, handling authentication, login flows, consent records, and loyalty/purchase-history profile data. A key to that infrastructure, not an analytics key, ships verbatim in every installed APK. com.emarsys.geofence.RegisterGeofencesOnBootCompletedReceiver registers location-based marketing geofence zones at system boot, before the app has ever been opened and before any consent screen exists (H1): once a device enters a roughly 200-metre radius around a SPAR store, this can trigger push marketing based on standing location surveillance that began before the user ever interacted with the app. SPAR's own code implements a dedicated plus.spar.si.api.contacts.ReadPhoneContactsTask class (H2), tied to a shopping-list-sharing feature, giving a supermarket loyalty app access to the phone contacts of people who are not themselves SPAR users and have given no consent of their own. Finally, FirebaseInitProvider initializes before consent (initOrder=100) alongside the Android Privacy Sandbox's ACCESS_AD SERVICES_ATTRIBUTION and ACCESS_AD SERVICES_AD_ID permissions (H3).

RFI-IRFOS disclosed these findings on 2026-06-30 to security@spar.si and zasebnost@spar.si, with odnosi-z-javnostmi@spar.si CC'd. zasebnost@spar.si and odnosi-z-javnostmi@spar.si hard-bounced immediately and on every subsequent attempt; a later attempt to reach dpo@spar.si on 2026-07-27 also hard-bounced. security@spar.si, the one address that accepted every one of the nine messages sent over 109 days without a single bounce, never replied once, not with an automated acknowledgment and not with a substantive response. The embargo deadline, fixed at 2026-09-28 in the original disclosure, was reached and passed with zero engagement of any kind from SPAR. This report publishes 19 days past that embargo.

ID	Severity	Title
C1	CRITICAL	Two Firebase keys, a Google Maps key, and the production database URL hardcoded in the distributed binary
C2	CRITICAL	SAP Gigya (CIAM) API key hardcoded: identity, login, and consent-management infrastructure exposed
H1	HIGH	Emarsys geofence registration at system boot: location-based marketing before the app is opened and before any consent

ID	Severity	Title
H2	HIGH	ReadPhoneContactsTask in SPAR's own code: third-party contact data read for a shopping-list-sharing feature
H3	HIGH	Firebase pre-consent initialization plus Android Privacy Sandbox attribution and advertising-ID permissions

Subject & Operator Context

SPAR d.o.o., Ljubljana operates the SPAR Plus loyalty and shopping app for the Slovenian retail market, as part of the SPAR International group headquartered in Salzburg, Austria. This audit covers the Android application (plus.spar.si) available on Google Play. A supermarket loyalty app combines three categories of data that are individually sensitive and, together, form a detailed behavioral profile: purchase history (via the loyalty program), location (via store-proximity geofencing), and, through this app's own code, the contact lists of people outside the app's own user base entirely.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 2026-06-30 to security@spar.si and zasebnost@spar.si, with odnosi-z-javnostmi@spar.si CC'd and the Informacijski pooblaščenec (IP, Slovenia's data protection authority and SPAR d.o.o.'s lead supervisory authority), the Austrian DSB, CERT.at, and the EDPS copied. zasebnost@spar.si and odnosi-z-javnostmi@spar.si both hard-bounced on this first attempt, address unknown.

A follow-up on 2026-07-06 to the same two bounced addresses confirmed the bounce again. The follow-up of 2026-07-17 noted explicitly that no reply had come from SPAR itself, only the automatic receipt confirmations the Slovenian regulator's intake system generates on every CC'd message (which state in their own text that they are automated and should not be replied to). On 2026-07-27, having confirmed both original direct addresses dead, RFI-IRFOS additionally tried dpo@spar.si, which also hard-bounced. Five further follow-ups (2026-08-05, 2026-08-15, 2026-08-24, 2026-08-31, 2026-09-12) were sent to security@spar.si, the one address that had accepted every message without a single bounce across the entire engagement. Not one of those nine total messages ever drew a reply from SPAR, automated or substantive. The embargo deadline, fixed at 2026-09-28 in the original disclosure, was reached and passed with zero of the three repeated questions answered.

Findings

C1: Two Firebase keys, a Google Maps key, and the production database URL hardcoded in the distributed binary

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N, 9.1 — four separate credentials for the same production project ship verbatim in every installed copy

```
google_api_key:      [REDACTED IN PUBLIC REPORT -- disclosed privately to SPAR in R1  
                      ]  
google_crash_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to SPAR in R1  
                      ] (identical value)  
google_maps_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to SPAR in R1  
                      ]  
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to SPAR in R1  
                       ]
```

All four values present verbatim in every installed copy of plus.spar.si.
Zero reply received across nine messages over 109 days.

Impact: res/values/strings.xml hardcodes four separate credentials for the same production Firebase project [REDACTED IN PUBLIC REPORT – disclosed privately to SPAR in R1]: a google_api_key, an identical google_crash_api_key, a separate google_maps_api_key, and the production firebase_database_url itself. All four are present verbatim in every installed copy of plus.spar.si and extractable with free, widely available tooling in under a minute. This combination creates both a quota-exhaustion/denial-of-service surface across two separate Google Cloud products (Firebase and Maps) and, should the database security rules be misconfigured, a direct read/write path into SPAR's production customer database. SPAR has not replied to any of nine messages across 109 days; the configuration remains exactly as first identified, with no acknowledgment, no date, and no remediation of any kind.

C2: SAP Gigya (CIAM) API key hardcoded: identity, login, and consent-management infrastructure exposed

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 — a key to the identity and consent-management platform behind the SPAR customer account system ships verbatim in every installed copy

```
gigya_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to SPAR in R1]  
gigya_api_domain: eu2.gigya.com
```

Gigya manages: user authentication/login flows, consent records, customer profile data (loyalty, purchase history), SSO token issuance. Key present verbatim in every installed copy of plus.spar.si. Zero reply received across nine messages over 109 days.

Impact: SAP Gigya is the Customer Identity and Access Management (CIAM) platform behind the entire SPAR customer account system: it handles user authentication and login flows, consent-record storage, and customer profile data including loyalty status and purchase history, and issues SSO tokens. The Gigya API key and API domain (eu2.gigya.com) are hardcoded in res/values/strings.xml [REDACTED IN PUBLIC REPORT – disclosed privately to SPAR in R1], present verbatim in every installed copy of plus.spar.si. This is not an analytics key; it is a key to the identity and consent infrastructure itself, and anyone who decompiles the APK can authenticate directly against eu2.gigya.com with it, with the potential to query identity data, read or manipulate consent records, or execute login flows on behalf of the app. SPAR has not confirmed, disputed, or named this finding across nine messages over 109 days, and has not stated whether the Informacijski pooblaščenec was notified under Art. 33 GDPR.

H1: Emarsys geofence registration at system boot: location-based marketing before the app is opened and before any consent

HIGH, 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, 7.3 — standing location surveillance for push marketing begins at device boot, before the user has ever opened the app

```
com.emarsys.geofence.RegisterGeofencesOnBootCompletedReceiver
    android:name="android.intent.action.BOOT_COMPLETED"
com.emarsys.mobileengage.geofence.GeofenceBroadcastReceiver
    android:name="com.emarsys.sdk.GEOFENCE_ACTION"
com.emarsys.EmarsysSdkInitializer (via androidx.startup) -- 636 smali classes
```

SPAR's reply record: zero, across nine messages over 109 days.

Impact: com.emarsys.geofence.RegisterGeofencesOnBootCompletedReceiver registers Emarsys marketing-automation geofence zones at BOOT_COMPLETED, before the user has opened the app for the first time and before any consent mechanism can be presented. Once registered, entering a defined zone (store-proximity radius) around a SPAR location can trigger push-marketing notifications, meaning the location surveillance this depends on is standing and continuous rather than tied to active app use. com.emarsys.EmarsysSdkInitializer additionally initializes via androidx.startup ahead of the consent screen. SPAR has not named, confirmed, or disputed this finding across nine messages over 109 days.

H2: ReadPhoneContactsTask in SPAR's own code: third-party contact data read for a shopping-list-sharing feature

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, 6.5 — contacts of people outside SPAR's own user base are read by a shopping-list-sharing feature with no documented legal basis for their data specifically

```
smali_classes6/plus/spar/si/api/contacts/ReadPhoneContactsTask.smali
Context: shoppinglist/share/ (shopping-list-sharing feature)
```

Data subject: contacts of people who are not themselves SPAR app users.
SPAR's reply record: zero, across nine messages over 109 days.

Impact: SPAR implements a dedicated plus.spar.si.api.contacts.ReadPhoneContactsTask class, tied to a shopping-list-sharing feature (shoppinglist/share/). RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.5 to HIGH because the people whose contact data this reads are, by definition, not SPAR app users themselves, they are third parties who have given no consent of their own to a supermarket loyalty app processing their name and contact details. A shopping-list-sharing feature in a retail loyalty app is not an obviously necessary context for reading a user's full phone contact list, and SPAR has not named, confirmed, or disputed this finding, or stated the Art. 6(1) legal basis for processing third-party contact data this way, across nine messages over 109 days.

H3: Firebase pre-consent initialization plus Android Privacy Sandbox attribution and advertising-ID permissions

HIGH, 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, 7.1 — tracking infrastructure initializes before any consent screen, alongside device-level advertising attribution permissions

```

FirebaseInitProvider (initOrder=100)    -- before any Activity, before consent
ACCESS_AD SERVICES_ATTRIBUTION         -- Android Privacy Sandbox Attribution
ACCESS_AD SERVICES_AD_ID               -- Android Advertising ID

```

SPAR's reply record: zero, across nine messages over 109 days.

Impact: FirebaseInitProvider initializes with initOrder="100", ahead of any Activity and therefore ahead of any consent dialog, identical in kind to the pre-consent pattern found across this campaign's Android findings. plus.spar.si additionally declares android.permission.ACCESS_AD SERVICES_ATTRIBUTION and android.permission.ACCESS_AD SERVICES_AD_ID, the Android Privacy Sandbox's attribution and advertising-ID permissions, meaning device-level ad-attribution infrastructure is present and available to initialize before consent alongside Firebase. SPAR has not named, confirmed, or disputed this finding across nine messages over 109 days.

Impact Analysis

These five findings form a single risk picture rather than five unrelated issues. C2's exposed Gigya CIAM key means the identity and consent-management layer behind every SPAR customer account is reachable with a key shipped in the public APK. C1's exposed Firebase/Maps credentials and production database URL sit on the analytics and crash-reporting layer of the same app. H1's boot-time geofence registration and H3's pre-consent Firebase/attribution initialization mean location and advertising-attribution tracking both begin before the user has made any consent decision at all. H2's contacts access extends the app's data footprint to people who have never used SPAR Plus and were never asked. Taken together: a supermarket loyalty app's identity infrastructure, location-tracking infrastructure, and third-party contact data are each one extracted credential or one undisclosed processing purpose away from a documented compliance or security incident, and SPAR has not engaged with any single piece of this picture across more than three months of outreach.

The Complete Chain: Nine Messages Across 109 Days, Zero Replies Of Any Kind

2026-06-30: RFI-IRFOS sends the full disclosure to security@spar.si and zasebnost@spar.si, odnosi-z-javnostmi@spar.si CC'd, the Informacijski pooblaščenec (IP, Slovenia), the Austrian DSB, CERT.at, and the EDPS copied. Both zasebnost@spar.si and odnosi-z-javnostmi@spar.si hard-bounce immediately. Embargo deadline established: 2026-09-28.

2026-07-06: First follow-up, sent to the same addresses. Both bounce again, confirming the addresses are dead, not a one-time delivery fault.

2026-07-17: Second follow-up. 17 days of silence noted; only the Slovenian regulator's automated receipt confirmations have arrived, explicitly marked in their own text as automated and not to be replied to.

2026-07-27: Third follow-up. Having confirmed both original direct SPAR addresses dead, RFI-IRFOS tries dpo@spar.si for the first time. It also hard-bounces.

2026-08-05: Fourth follow-up, to security@spar.si, the one address that has never bounced. 30 days since the previous message.

2026-08-15: Fifth follow-up, fifth repetition of the three open questions.

2026-08-24: Sixth follow-up, 55 days since the original disclosure, the Gigya CIAM key finding restated by name.

2026-08-31: Seventh follow-up, 62 days since the original disclosure.

2026-09-12: Eighth and final follow-up, 74 days since the original disclosure, 68 days since the last message that drew any response of any kind (none ever did). Three questions repeated a final time with a 2026-09-19 answer deadline.

Across nine total messages over 109 days, security@spar.si accepted every one without a single bounce and replied to none of them. The embargo deadline, fixed at 2026-09-28, was reached and passed with zero of the three questions answered and zero of the five findings named individually by SPAR.

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent. Two of three addresses bounce immediately. Embargo fixed at 2026-09-28.

2026-07-06 First follow-up, same two addresses bounce again.

2026-07-17 Second follow-up. Only automated regulator receipts received, no SPAR reply.

2026-07-27 Third follow-up, dpo@spar.si tried for the first time, also bounces.

2026-08-05 Fourth follow-up, to the one surviving address, security@spar.si.

2026-08-15 Fifth follow-up.

2026-08-24 Sixth follow-up.

2026-08-31 Seventh follow-up.

2026-09-12 Eighth and final follow-up, new answer deadline of 2026-09-19 set.

2026-09-28 Embargo date reached. No reply of any kind ever received from SPAR.

2026-10-17 This report published, 19 days after embargo. All five findings unaddressed.

Data Protection — Article by Article

Art. 32(1)(b) GDPR — Integrity and confidentiality of processing: both C1's Firebase/Maps credential exposure and C2's Gigya CIAM key exposure fall below the technical security measures this article requires, with C2 implicating the confidentiality and integrity of SPAR's entire customer identity and consent-management layer.

Art. 25 GDPR — Data protection by design and by default: C2's hardcoded CIAM credential in a publicly distributed binary is a design-stage failure in the identity infrastructure itself, not a runtime incident.

Art. 33 GDPR — Notification of a personal data breach: C2's exposure of identity-infrastructure credentials raises the question of whether the Informacijski pooblaščenec was notified; SPAR has not answered this question across nine messages.

Art. 7 GDPR — Conditions for consent: H1's boot-time geofence registration and H3's pre-consent Firebase/attribution initialization both begin before any consent mechanism exists.

Art. 6(1) GDPR — Lawfulness of processing: neither H1's geofence-based location tracking nor H2's third-party contacts access has a stated legal basis in any SPAR reply.

Art. 5(1)(c) GDPR — Data minimization: H1's standing, boot-time location surveillance for marketing purposes exceeds the data minimization principle relative to its stated purpose.

Art. 13 GDPR — Information to be provided: H2's contacts access affects data subjects (the contacts themselves) who are not SPAR users and have received no transparency information of any kind from SPAR.

Regulatory Landscape & Fine Exposure

SPAR d.o.o. is registered in Ljubljana, Slovenia, placing it under the jurisdiction of the Informacijski pooblaščenec (IP), which has been copied on every message in this disclosure. As the Slovenian operating entity of a retail group headquartered in Salzburg, Austria, SPAR d.o.o. is subject to the full GDPR Article 83 fine structure.

Art. 83(5) GDPR — Maximum fines up to EUR 20,000,000 or 4% of worldwide annual turnover — applies to violations of Art. 5 (principles, implicated by H1), Art. 6 (lawfulness, implicated by H1 and H2), Art. 7 (conditions for consent, implicated by H1 and H3), and Art. 25 (data protection by design, implicated by C2).

Art. 83(4) GDPR — Maximum fines up to EUR 10,000,000 or 2% of worldwide annual turnover — applies to violations of Art. 32 (security of processing), implicated by both C1 and C2, and Art. 33 (breach notification), implicated by the unanswered question in C2.

Three of the four email addresses RFI-IRFOS attempted for this disclosure (zasebnost@spar.si, odnosi-z-javnostmi@spar.si, dpo@spar.si) were hard-bounced and non-functional throughout the entire 109-day engagement period, a basic intake-channel failure independent of the technical findings themselves.

Indicators of Compromise

All findings derive from static analysis of the plus.spar.si production APK as published on Google Play, analyzed 2026-06-30. No SPAR servers, accounts, or infrastructure were probed.

Residual Risk & Recommendations

C1 – Hardcoded Firebase/Maps credentials: Rotate all four exposed credentials. Confirm Firebase Security Rules deny anonymous read/write by default on the production database.

C2 – Hardcoded Gigya CIAM key: Rotate the exposed key immediately given its scope (identity, login, consent records). Confirm whether the Informacijski pooblaščenec requires notification under Art. 33 GDPR for this configuration and, if so, complete it.

H1 – Boot-time geofence registration: Defer Emarsys geofence zone registration and EmarsysSdkInitializer until after a consent decision has been made, rather than at BOOT_COMPLETED.

H2 – Contacts access: Document the specific Art. 6(1) legal basis for reading the phone contacts of people who are not SPAR users, and ensure the shopping-list-sharing feature's privacy disclosure specifically names this processing rather than relying on a general permissions disclosure.

H3 – Pre-consent Firebase/attribution initialization: Gate FirebaseInitProvider and the Privacy Sandbox attribution/advertising-ID permissions behind the consent decision rather than initializing at process start.

Process-level: Three of the four contact addresses used for this disclosure were non-functional for the entire 109-day engagement. A functioning, monitored security and data-protection contact address is itself a basic requirement independent of any of the five technical findings above.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of plus.spar.si, the production APK as published on Google Play, analyzed 2026-06-30, using publicly available tools (apktool, jadx, jq). No SPAR servers, accounts, or production infrastructure were probed or accessed. Technical evidence is archived under chain of custody and will be provided to the Informacijski pooblaščenec on request. Research conducted under GDPR Art. 89 (scientific research exemption), ISO/IEC 29147 (coordinated disclosure standard), and the Austrian Federal Constitutional Law Art. 17 (freedom of research). REF PLUS.SPAR.SI.