Security & Privacy Disclosure, Final Report

Life360 (com.life360.android.safetymapd)

A family location app that starts two driving data vendors before any consent screen and describes an opt-out advertising program that shares data with third parties, with an operator that replied twice and answered one of three questions.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 21 NOVEMBER 2026. OPERATOR REPLIED TWICE (11 AND 29 SEPTEMBER 2026), TWO QUESTIONS OPEN, EIGHT FINDINGS UNANSWERED.

Target	Life360, Inc., Life360 (Android app)
Version Audited	26.31.0 / versionCode 2914950 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	8: 2 High, 5 Medium, 1 Low (none of them in the notice)
Status	REPLIED 2026-09-11 AND 2026-09-29, TWO QUESTIONS OPEN AS OF 21 NOVEMBER 2026, NO REPLY TO THE EIGHT FINDINGS
SHA-256 (base APK)	`b7a4e58e3e26dbd2d983cbc85c1f2853cf69e664453e6ab68f44878a294c7b14`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Engagement Summary 6

6 Findings 7

6.1 C1: The app's own screens describe an advertising program that shares user data with third parties for their own commercial use, controlled by an opt-out, and the GDPR variant reuses the US text . . . 7

6.2 C2: Two driving and location data vendors, Arity and Sentiance, start with the process and the boot event, and no consent platform exists in the package . . 9

6.3 H1: Pangle of ByteDance and Mintegral are compiled into the advertising mediation stack . . . 10

6.4 H2: Endpoints for Unified ID 2.0 and its EU instance EUID are hardcoded in the app . . . 11

6.5 H3: Plaid for bank account linking and Persona for government ID and facial liveness checks are wired to the paid identity theft protection tier . . . 12

6.6 H4: The app derives driving events, trip analyses and sleep states on the device, and an intent action named RAW_DATA_EXCHANGE sits next to the Arity engine . . . 13

6.7 M1: Five distinct Google API keys and a legacy Firebase Realtime Database URL ship in every copy of the app . . . 14

6.8 M2: No certificate pinning, and a network security configuration that holds only a debug trust anchor . . . 15

7 Impact Analysis 15

8 The Complete Chain 16

9 Child Protection 16

10 Data Protection: Article by Article 17

11 Platform Accountability & DSA 17

12 Regulatory & Legal Landscape 18

13 Indicators of Compromise & Reproducible Evidence 19

14 Disclosure Timeline & Outcome 20

15 What Was Done Well 20

16 Residual Risk & Recommendations 21

Executive Summary

Life360 is a family location sharing and safety platform of Life360, Inc. in San Francisco, listed on Nasdaq and the ASX, with more than 100 million installs on Google Play. Members of a family circle see each other's location, driving reports and safety alerts, and paid tiers add identity theft protection. On 23 August 2026 RFI-IRFOS sent a notice with REF LIFE360-2026-R1 to privacy@life360.com with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy. The notice carried three points that differ from the findings of the full analysis. It named the missing representative and officer, the household graph question and the missing support address. None of the eight findings in this report was part of the notice.

A root level code analysis of version 26.31.0 shows that the app's own screens describe an advertising program that shares user data with third parties for their own commercial use, controlled by an opt-out, and that the screen for the GDPR variant reuses the US text (C1). The Arity and Sentiance driving and location vendors start with the process and the device boot, and no consent platform exists in the package (C2). Further findings cover Pangle and Mintegral in the mediation stack (H1), the Unified ID 2.0 and EUID endpoints (H2), Plaid and Persona for the paid tier (H3), derived driving and sleep states (H4), five hardcoded Google keys (M1) and the missing certificate pinning (M2).

A reassessment by CVSS v4.0 band puts two findings at High, five at Medium and one at Low. The Critical labels of C1 and C2 of the working analysis move to High. The High labels of H1 to H4 move to Medium, and M2 moves from Medium to Low. Each change is stated in the open items with its reason. The operator's own text credits the under 18 carve-out from targeted advertising, and the app declares itself a monitoring tool.

The operator replied on 11 September 2026 and on 29 September 2026 from legal@life360.com. It named an Art. 27 representative, Osano International Compliance Services Limited in Dublin, and the notice point on the representative is withdrawn. It stated that data protection impact assessments are carried out for the core application and the Circle and location features and that it does not share them. It did not answer the yes or no question on sharing of household data. Two questions remain open on 21 November 2026. The eight findings of this report were not in the first notice. RFI-IRFOS stated all eight to the operator on 15 November 2026 with C1, C2, H1 to H4, M1 and M2 in the severities of this report, together with the two open questions. Nothing has arrived since, apart from an automated confirmation of the same day.

Scope: Root level code analysis of the Google Play release 26.31.0 (versionCode 2914950) of Life360, obtained as the universal base.apk, 104.8 MB, from an APKMirror split bundle (release id 15533562). Two other mirrors showed tab hijacking in the browser and were abandoned. Work done: manifest and resource decode with apktool without source decode, extraction of the 8 classes dex files of about 85 MB, and string search over all of them. A first full decode ran out of disk space and was replaced by direct extraction of the dex files. No full bytecode disassembly was done, so code level statements rest on strings and are marked accordingly. The Google Play listing with the Data Safety card was verified on 23 August 2026. The app was not installed, no account was created, no operator server was called and no traffic was captured. The privacy policy of the operator was not re-read for this report. The operator's statements about it come from its reply of 29 September 2026. Findings that depend on runtime behaviour are marked as such.

ID	Severity	Title
C1	HIGH	The app's own screens describe an advertising program that shares user data with third parties for their own commercial use, controlled by an opt-out, and the GDPR variant reuses the US text
C2	HIGH	Two driving and location data vendors, Arity and Sentiance, start with the process and the boot event, and no consent platform exists in the package
H1	MEDIUM	Pangle of ByteDance and Mintegral are compiled into the advertising mediation stack
H2	MEDIUM	Endpoints for Unified ID 2.0 and its EU instance EUID are hardcoded in the app
H3	MEDIUM	Plaid for bank account linking and Persona for government ID and facial liveness checks are wired to the paid identity theft protection tier
H4	MEDIUM	The app derives driving events, trip analyses and sleep states on the device, and an intent action named RAW_DATA_EXCHANGE sits next to the Arity engine
M1	MEDIUM	Five distinct Google API keys and a legacy Firebase Realtime Database URL ship in every copy of the app
M2	LOW	No certificate pinning, and a network security configuration that holds only a debug trust anchor

Finding Status at a Glance

ID	Disclosed	This report	State on 21 November 2026
C1	Not in notice	HIGH	Toggle default and recipients not verified.
C2	Not in notice	HIGH	Sampling at start not determined.
H1	Not in notice	MEDIUM	Enablement and payload not verified.
H2	Not in notice	MEDIUM	Calling code not traced.
H3	Not in notice	MEDIUM	Use in the Union not verified.
H4	Not in notice	MEDIUM	Raw data path not verified.
M1	Not in notice	MEDIUM	Rules and restrictions not tested.
M2	Not in notice	LOW	Contextual note.
N1	HIGH	Withdrawn in part	Art. 27 representative is named in policy section VIII.c.ii. Credited. DPO still not named.
N2	HIGH	Not confirmed	Household graph not found in the package. Question 2 and question 3 open.
N3	MEDIUM	Not a finding	privacy@life360.com is in the package strings. The notice reached the operator.

The notice of 23 August 2026 carried three points, N1 to N3, that are not findings of this report. C1 to M2 are the findings of the full analysis and none was in the notice, so the column Disclosed shows Not in notice and the severity of the working analysis is the old label of each change. This report uses the CVSS v4.0 band of each finding. C2 stays High through a blast-radius escalation that the finding states. A downgrade is made only where the evidence in the package does not carry the earlier label.

Subject & Operator Analysis

The operator is Life360, Inc., San Francisco, California, listed on Nasdaq under LIF and on the ASX. The Play listing shows more than 100 million downloads, the content rating PEGI 3 with the descriptors Users Interact, Shares Location and Digital Purchases, and a stated user base of more than 66 million. The contacts are privacy@life360.com, which the strings confirm, and the help center at support.life360.com. No direct support or press address was found in the package. The operator answered from legal@life360.com.

The operator names an Art. 27 representative for the Union and the United Kingdom in section VIII.c.ii of its privacy policy, in its reply of 29 September 2026: Osano International Compliance Services Limited, ATTN 4XK3, 3 Dublin Landings, North Wall Quay, Dublin 1, D01C4E0, and Osano UK Compliance LTD, ATTN 4XK3, 42-46 Fountain Street, Belfast, Antrim, BT1 5EF. This closes the representative point of the notice. No data protection officer was named in the replies. No main establishment in the Union is identified, so the one-stop-shop mechanism does not apply and the Austrian Datenschutzbehörde can receive complaints directly.

The product has a first-party relationship graph, the Circle, in which users join a group to see each other. It is the declared product. The analysis found no hidden co-location inference beyond it.

Architecture & Data Flow

The app is native Android in Java and Kotlin with 8 classes dex files of about 85 MB, minimum SDK 29 and target SDK 35. The permissions include fine, coarse and background location, camera, microphone, contacts, phone state, call, Bluetooth scan, advertise and connect, activity recognition, biometric and fingerprint use, and the advertising ID and the three ad services permissions. READ_USER_DICTIONARY is present and no feature for it was identified.

The data side has four parts. The first is the driving and location engines Arity and Sentiance (C2, H4). The second is a wide advertising and attribution stack with AppLovin, Google AdMob, Meta Audience Network, Vungle, Unity Ads, ironSource, InMobi, Moloco, Pangle, Mintegral, AppsFlyer and Branch (C1, H1). The third is identity linkage through UID2 and EUID, and analytics with EU region endpoints for Amplitude, api.eu.amplitude.com and regionconfig.eu.amplitude.com (H2). The fourth is the paid tier with Plaid and Persona (H3). Sentry automatic start is switched off.

The backend side is not visible. Which servers, regions and retention periods apply was not observed, and no traffic was captured.

Engagement Summary

The notice REF LIFE360-2026-R1 was sent on 23 August 2026 at 12:19 UTC from rfi.irfos@gmail.com to privacy@life360.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried three points and three questions on the representative and officer, on sharing of household data and on an impact assessment, and set the embargo date of 21 November 2026. On 11 September 2026 at 19:05 UTC the Life360 Legal Team replied from legal@life360.com with pointers to sections of the privacy policy and a statement on impact assessments. RFI-IRFOS answered on the same day at 19:23 UTC, asked for the name of the representative, a yes or no on sharing and a confirmation on the impact assessment, and set 25 September 2026. On 29 September 2026 at 16:23 UTC the operator named the representative and said that questions 2 and 3 had been answered. RFI-IRFOS replied at 17:55 UTC, credited the answer on question 1, and restated the two open questions. On 15 November 2026 at 14:02 UTC RFI-IRFOS sent a supplementary notice six days before publication to legal@life360.com and privacy@life360.com. It stated the eight findings of this report for the first time, withdrew the contact address point, closed the representative point and restated questions 2 and 3. The privacy mailbox returned an automated confirmation of the privacy request at 14:02 UTC. No substantive message from the operator followed, and no delivery failure was returned.

Findings

C1: The app's own screens describe an advertising program that shares user data with third parties for their own commercial use, controlled by an opt-out, and the GDPR variant reuses the US text

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.1 (CVSS-B), first stated in this report

The file res/values/strings.xml holds a set of privacy choice strings. One says that Life360 has an advertising program that may use or share personal information to personalise the ad experience on third-party sites or applications. One says the user can direct Life360 not to sell data to third parties for their commercial use or to share it for targeted advertising. One bullet says Life360 will stop sharing data with third parties for their own commercial use. A toggle is labelled Enable personalized ads outside of Life360. A further string says that Nativo, an advertising technology company, is now part of Life360. The string for the GDPR variant of the screen carries the same body text as the US variant. The control is an opt-out, so the user directs Life360 to stop and does not give permission to start. The Data Safety card of the Play listing, verified on 23 August 2026, says the app may share location and health and fitness data with third parties. The default state of the toggle for accounts in the Union is UNVERIFIED from static resources, and so are the recipients.

```
[line 5361] privacy_choices_body_ad_program:
"Life360 has an advertising program that may use or share your personal information
("data") to personalize your ad experience on third-party sites or applications."

[line 5363] privacy_choices_body_intro:
"You can direct us to not sell your data to third parties for their commercial use
or to share it for purposes of "targeted advertising.""

[line 5366] privacy_choices_bullet_commercial_use:
"We will stop sharing your data with third parties for their own commercial use."

[line 5375] privacy_choices_personalized_ads_body_intro_gdpr:
"You can direct us to not sell your data to third parties for their commercial use
or to share it for purposes of "targeted advertising.""

[line 5374] privacy_choices_nativo_blurb:
"Nativo, an advertising technology company, is now a part of Life360. Learn more
about these services or opt out here."

[line 5380] privacy_choices_personalized_ads_toggle_label: "Enable personalized ads
    outside of Life360"
```

```
"This app may share these data types with third parties: Location and Health and
    fitness"
"This app may collect these data types: Personal info, Messages and 5 others."
```

The operator has a stated credit that applies here. The strings say the operator does not sell or share information for targeted ads if it knows a member is under 18, in the standard and in the GDPR variants.

Impact: A family location product, whose function is continuous location of the members of a circle, describes in its own screens a program that shares data with third parties for their commercial use and offers an opt-out for it. Consent under Art. 6(1)(a) and Art. 7 is given before the processing starts, and an opt-out screen written for the US framework does not establish it by itself. The affected group is the adult and teenage members of family circles who use the app. Members under 18 are carved out of targeted advertising in the operator's own text.

Fix: State the default of the toggle for accounts in the Union, name the categories and recipients, and move the sharing for third parties' own commercial use to opt-in consent.

C2: Two driving and location data vendors, Arity and Sentiance, start with the process and the boot event, and no consent platform exists in the package

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 (CVSS-B), first stated in this report, rated HIGH by blast-radius escalation

The manifest declares androidx.startup.InitializationProvider with init order 109, and its initializer list names com.arity.coreengine.driving.CoreEngineInitializer. Android runs content providers during application creation, before any activity, so the Arity driving engine bootstraps at every cold start. The Sentiance SDK has a boot completed receiver for QUICKBOOT_POWERON and BOOT_COMPLETED and declares the features CrashDetectionFeature, DrivingInsightsFeature and EventTimelineFeature. The dex files hold five hardcoded endpoints, api.arity.com, api-staging.arity.com, tracking.arity.com, tracking-staging.arity.com and api.sentiance.com. The Arity package accounts for 909 string occurrences and the Sentiance package for 1,686 across the eight dex files. The native library libsentiance_breakpad.so is bundled. A search of all eight dex files for OneTrust, Didomi, Usercentrics, ConsentManager, Sourcepoint, Quantcast and the Google User Messaging Platform returned no match. The only consent related strings are the IAB TCF key names and an isUserSubjectToGDPR flag read by the AppsFlyer SDK, which read a value that a consent platform would set. Whether the Arity initializer starts sampling at once or registers listeners that wait for a later consent or subscription flag was not determined without a control-flow review or a dynamic trace. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the app has more than 100 million installs, the vendors are built for driving and location data, and family circles include minors.

```
<provider android:authorities="com.life360.android.safetymapd.androidx-startup"
          android:exported="false" android:initOrder="109"
          android:name="androidx.startup.InitializationProvider">
    <meta-data android:name="androidx.lifecycle.ProcessLifecycleInitializer" android:
    value="androidx.startup"/>
    <meta-data android:name="com.arity.coreengine.driving.CoreEngineInitializer"
    android:value="androidx.startup"/>
</provider>

<receiver android:exported="false" android:name="com.sentiance.sdk.
    BootCompletedReceiver">
    <intent-filter>
        <action android:name="android.intent.action.QUICKBOOT_POWERON"/>
        <action android:name="android.intent.action.BOOT_COMPLETED"/>
    </intent-filter>
</receiver>
<meta-data android:name="com.sentiance.sdk.feature.CrashDetectionFeature" android:
    value=""/>
<meta-data android:name="com.sentiance.sdk.feature.DrivingInsightsFeature" android:
    value=""/>
<meta-data android:name="com.sentiance.sdk.feature.EventTimelineFeature" android:value
    =""/>
```

```
https://api.arity.com          https://api-staging.arity.com
https://tracking.arity.com     https://tracking-staging.arity.com
https://api.sentiance.com
lib/arm64-v8a/libsentiance_breakpad.so
```

Impact: The Arity vendor is built for driving data for the insurance sector. Two vendors for driving and location data are wired to the start of the process and to the boot of the device, and the package holds no consent platform that could gate them. The users are the members of family circles, which include minors added by a parent. A member cannot decline start-up processing from inside the app.

Fix: Start Arity and Sentiance only after a consent decision for the user, and document the legal basis for the start-up processing of members of a circle.

H1: Pangle of ByteDance and Mintegral are compiled into the advertising mediation stack

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), first stated in this report

The dex files hold the Pangle classes TTAdActivity, TTFullScreenVideoActivity, the PAG interstitial, banner, native and reward classes and PangleEncryptManager, and the Mintegral classes DomainMBCommonActivity, MBConfiguration and the reward video classes. They sit in a wider mediation stack with AppLovin, Google AdMob, Meta Audience Network, Vungle, Unity Ads, ironSource, InMobi and Moloco, and AppsFlyer and Branch for attribution. No endpoint in the PRC was found in the dex string tables, which fits the documented encrypted transport of Pangle. Whether these networks are enabled in the waterfall for accounts in the Union, and what payload reaches them, was not confirmed statically.

```
com.bytedance.sdk.openadsdk.activity.TTAdActivity
com.bytedance.sdk.openadsdk.activity.TTFullScreenVideoActivity
com.bytedance.sdk.openadsdk.api.interstitial.PAGInterstitialAd
com.bytedance.sdk.openadsdk.api.banner.PAGBannerAd / api.nativeAd.PAGNativeAd / api.
    reward.PAGRewardedAd
com.bytedance.sdk.component.embedapplog.PangleEncryptManager
com.mbridge.msdk.activity.DomainMBCommonActivity
com.mbridge.msdk.out.MBConfiguration / MBRewardVideoHandler / reward.player.
    MBRewardVideoActivity
```

Impact: Advertising identifiers and location adjacent data of the users of a family location app could reach ad networks whose operators are based in the PRC if the networks are enabled. A transfer assessment would have to cover that country. The integration is proven, and the flow is not.

Fix: State which networks are enabled for accounts in the Union, name the transfer mechanism, and remove networks that are not needed.

H2: Endpoints for Unified ID 2.0 and its EU instance EUID are hardcoded in the app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), first stated in this report

The dex files hold the endpoints https://prod.uidapi.com, the production endpoint of Unified ID 2.0 of The Trade Desk, and https://prod.euid.eu, the EU instance of the same system. These systems turn a hashed email address or phone number into a portable identifier that advertising partners can match against their own records, independent of the Google advertising ID. The EU endpoint indicates that the mechanism is meant to operate for users in the Union. The calling code was not traced, so whether it runs, and which identifier it sends, are UNVERIFIED.

```
https://prod.uidapi.com
https://prod.euid.eu
```

Impact: A mechanism built to link one person across publishers and apps is present in a family location app. If it is active, a member of a circle can be matched across the advertising ecosystem. The presence of the EU instance leaves no doubt that the Union market is intended.

Fix: State whether the identity linkage is active, which identifier it uses and the legal basis, and tie it to a consent decision.

H3: Plaid for bank account linking and Persona for government ID and facial liveness checks are wired to the paid identity theft protection tier

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.9 (CVSS-B), first stated in this report

The manifest holds a Plaid file provider, a redirect activity with the plaid scheme and the Plaid link activity, and a Persona document file provider and inquiry activity, with an ML Kit dependency for OCR, face and barcode detection. The endpoints in the dex strings are dashboard.plaid.com, production.plaid.com, sandbox.plaid.com, analytics.plaid.com, withpersona.com, webrtc-consumer.withpersona.com and inquiry-fallback.withpersona.com. The Plaid package accounts for 4,117 string occurrences and the Persona package for 4,604. The strings of the paid tier promise reimbursement of stolen funds up to 25,000 USD, dark web monitoring and identity theft restoration. Whether these flows run for accounts in the Union, or only in a paid tier of the United States market, was not confirmed. The integration is not a dormant library, because dedicated activities, providers and intent filters make it reachable.

```
<provider android:authorities="com.life360.android.safetymapd.com.plaid.link.internal.
    PlaidFileProvider"
          android:name="com.plaid.link.internal.PlaidFileProvider" .../>
<activity android:name="com.plaid.internal.LinkRedirectActivity" ...>
    <intent-filter><data android:scheme="plaid"/><data android:host="complete"/>
        <data android:host="redirect"/><data android:host="resume"/></intent-filter>
</activity>
<activity android:name="com.plaid.internal.link.LinkActivity" .../>

<provider android:authorities="com.life360.android.safetymapd.persona.provider"
          android:name="com.withpersona.sdk2.inquiry.DocumentFileProvider" .../>
<activity android:name="com.withpersona.sdk2.inquiry.internal.InquiryActivity" .../>
<meta-data android:name="com.google.mlkit.vision.DEPENDENCIES" android:value="ocr,face
    ,barcode"/>
```

```
dba_breach_report_upsell_point_1: "$25k USD reimbursement of stolen funds"
dba_resolve_desc: "We provide steps to avoid identity theft and secure your family's
    exposed info."
dba_safety_details_id_theft_turn_off_dialog_text: "Turning off ID Theft Protection
    will stop you
  from getting any reimbursement of stolen funds and 24/7 white-glove restoration
    support."
dba_welcome_description: "We'll let you know if we detect your family's email
    addresses or
  passwords on the dark web to avoid identity theft."
```

Impact: A family that buys the location product may not expect that the upgrade also routes bank account credentials to a US processor and a facial biometric check to another. Biometric data for identification is a special category under Art. 9, and the processors are in the United States. A data protection impact assessment would be expected for this combined processing.

Fix: State whether the identity protection flows are offered in the Union, name the Art. 9(2)

basis and the transfer mechanism for both processors, and publish the impact assessment.

H4: The app derives driving events, trip analyses and sleep states on the device, and an intent action named RAW_DATA_EXCHANGE sits next to the Arity engine

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), first stated in this report

The manifest declares a DriverBehaviorReceiver with the actions CRASH_DETECTED, RAW_DATA_EXCHANGE, SDK_STARTUP and TRIP_ANALYZED, and a SleepClassifyReceiver for the Morning Check-In feature. The native libraries include libtensorflowlite_jni.so for on-device inference. The paid tier copy names Individual Driver Reports and Family Driving Summary, so the derived states are shown as a product feature. A computed state such as asleep, awake or drove aggressively can be more revealing than a single location point. The action name RAW_DATA_EXCHANGE suggests that raw sensor data is exchanged with the driving engine. Whether it leaves the device toward the Arity backend is UNVERIFIED without a dynamic capture.

```
<receiver android:name="com.life360.android.driving.DriverBehaviorReceiver">
    <intent-filter>
        <action android:name="com.life360.android.safetymapd.DriverBehavior.
    CRASH_DETECTED"/>
        <action android:name="com.life360.android.safetymapd.DriverBehavior.
    RAW_DATA_EXCHANGE"/>
        <action android:name="com.life360.android.safetymapd.DriverBehavior.
    SDK_STARTUP"/>
        <action android:name="com.life360.android.safetymapd.DriverBehavior.
    TRIP_ANALYZED"/>
    </intent-filter>
</receiver>
<receiver android:name="com.life360.android.morningcheckin.wake.SleepClassifyReceiver
    "/>
lib/arm64-v8a/libtensorflowlite_jni.so
```

Impact: Derived behavioural states of the members of a family are retained and shown to other members. They need their own place in the data inventory, the retention schedule and the impact assessment, independent of the location points they are computed from.

Fix: List the derived states in the data inventory, state their retention, and say whether raw sensor data or the derived states reach Arity or its customers.

M1: Five distinct Google API keys and a legacy Firebase Realtime Database URL ship in every copy of the app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), first stated in this report

The file res/values/strings.xml holds a Google API key with the Firebase identifiers, and the manifest holds a maps key. Three further keys appear verbatim in the dex string tables, and their binding was not traced. Google documents such keys as identifiers and not as secrets, so the exposure is availability, through quota exhaustion. The legacy Realtime Database type is historically prone to loose security rules. RFI-IRFOS did not query the database, and the key restrictions and the rules are not visible from the package.

```
google_api_key           AIzaSyBnUX4_tM-D5bW3aPF3ysEyxU-pgt2hWtk
google_app_id            1:316780013370:android:0ac587c694541924
gcm_defaultSenderId      316780013370
project_id               life360.com:l360safetycenter
firebase_database_url    https://life360-com-l360safetycenter.firebaseio.com
com.google.android.geo.API_KEY  AIzaSyDJagPqPY8GrGF-enk_JChbGrxqeCLwP6s
```

```
Keys in the classes dex string tables, binding not traced:
AIzaSyAYoKdlkfrse-Jdj15fc_FI0bht0mX_YBs
AIzaSyBzmLWygDURw9zF3siSB_a5px5jsec4hLs
AIzaSyDVsc4mFJOXNAFkx46vQCNkv-DZMHEjsdU
```

Impact: Anyone can read the keys from the package. Exhausting the quota of the projects could slow or stop functions that depend on them. Whether the database holds personal data is not shown.

Fix: Restrict each key by package name and signing certificate, and review the rules of the Realtime Database.

M2: No certificate pinning, and a network security configuration that holds only a debug trust anchor

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), first stated in this report

The manifest sets usesCleartextTraffic to false, which is a correct and deliberate choice. The network security configuration holds only a debug-overrides block, which has no effect in a release build. It has no base configuration, no domain configuration and no pin set, so no certificate pinning exists for any endpoint, including the continuous location and driving channels. This is common practice and not a defect by itself. The finding is a contextual note.

```
<network-security-config>
    <debug-overrides>
        <trust-anchors>
            <certificates src="user" />
        </trust-anchors>
    </debug-overrides>
</network-security-config>
```

Impact: A party that controls the system trust store of a device or that sits on a network with an installed trusted certificate could read the traffic of the app. That needs control over the device or the network path.

Fix: Consider pinning for the endpoints that carry location and driving data.

Impact Analysis

The people affected are the members of family circles of the app, adults, teenagers and children added by a parent. The app has an age gate for children under 13 with a parental consent flow, and it states that it does not sell or share information for targeted ads if it knows a member is under 18.

The weight of the case sits at two points. The app’s own screens describe an advertising program that shares data with third parties for their own commercial use, and the control is an opt-out (C1). Two vendors for driving and location data start with the process and the boot of the device, and nothing in the package can gate them (C2).

What the package shows is labelled capability, text and file content. No location, driving or identity value was observed leaving a device, and the report asserts no such flow.

The Complete Chain

Step 1, install: a member installs the app. The Data Safety card says location and health and fitness data may be shared with third parties.

Step 2, start: at the first process start the Arity driving engine initialises through a startup provider and the Sentiance receivers are wired to the boot event, and the package holds no consent platform (C2).

Step 3, circle: the member joins a family circle. Location, driving reports and derived states such as sleep are shown to other members (H4).

Step 4, advertising: the privacy choices screen describes a program that shares data with third parties for their commercial use, controlled by an opt-out, with the US text reused for the GDPR variant (C1). Mediation networks include two with operators in the PRC (H1), and identity endpoints for UID2 and EUID are present (H2).

Step 5, paid tier: identity theft protection routes bank account linking to Plaid and a biometric check to Persona (H3).

Step 6, back end: five Google keys in every copy serve the projects (M1), and the traffic has no certificate pinning (M2).

Step 7, rights: the operator names a representative in the Union, says it carries out impact assessments and does not share them, and does not answer a yes or no on sharing of household data.

Child Protection

The group at the centre of this case is the minors who are members of a family circle, added by a parent. Children under 13 meet an age gate that asks a parent or legal guardian to say it is acceptable, which is a real consent flow. The operator’s text states that it does not sell or share information for targeted ads if it knows a member is under 18, in the standard and in the GDPR variants.

The open points are three. The vendors Arity and Sentiance start with the process, so the start-up processing covers the minors who are members, and nothing in the package gates it (C2). The age of digital consent in Austria is 14 under § 4 Abs. 4 DSG, and the operator’s age gate names 13 and 18 and does not mention it. The carve-out for under 18 members applies to targeted advertising and does not cover the driving and location vendors or the derived states of H4.

The Play rating PEGI 3 describes the content seen by the user and has no axis for continuous location of a minor. This report draws no conclusion from the number itself.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1 and C2.

Article 5(1)(c), data minimisation: engaged by H2 and H4.

Article 5(2), accountability: engaged by C2.

Article 6(1) and Article 7(1): engaged by C1 and C2. An opt-out is not consent in the sense of Art. 7, and the legal basis for the start-up processing is not stated.

Article 9: engaged by H3 for biometric data and, as a question, by H4 for sleep states. No processing of special categories by the operator is asserted beyond the integration.

Article 13 and Article 14: engaged by C1 for the recipients.

Article 25: engaged by M1 and H4.

Article 27: the operator named a representative in the Union in its reply of 29 September 2026, in section VIII.c.ii of its privacy policy. The point is closed.

Article 32(1)(a) and (b): engaged by M2 and M1.

Article 35: engaged by H3 and H4. The operator says that assessments exist for the core application and the Circle and location features and does not share them.

Articles 44 and 46: engaged by H1 and H3.

Platform Accountability & DSA

Google Play is an online platform under Regulation (EU) 2022/2065. Any person can submit a notice about an inaccurate Data Safety declaration under Art. 16 of that Regulation. RFI-IRFOS records the point here and treats the notice as a decision for the publication stage.

The Data Safety card of the Play listing, verified on 23 August 2026, says the app may share location and health and fitness data with third parties and may collect personal info, messages and five other categories. The card is consistent with C1 and is not contradicted by the package.

Regulatory & Legal Landscape

Life360, Inc., a company in San Francisco, offers Life360 to users in the Union through Google Play, so Art. 3(2) of the GDPR applies. No main establishment in the Union is identified, so the one-stop-shop mechanism does not apply and the supervisory authority of each Member State where users are affected is competent under Art. 55. The Austrian Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) received the notice in copy.

Infringements of Art. 5, 6, 7 and 9, of Art. 12 to 22 and of Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 25, 27 and 32 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82. Art. 5(3) of the ePrivacy Directive covers access to information on the user's device. The operator names an Art. 27 representative in Dublin, and the one-stop-shop mechanism still does not apply because no main establishment in the Union is identified. The notice of 23 August 2026 also cited Art. 33(4) as a question to the operator and no breach is asserted in this report.

The disclosure follows ISO/IEC 29147 and Art. 17 StGG. RFI-IRFOS acts under ZVR 1015608684 and GISA 39261441.

Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding. All values are given in full.

```
Package            com.life360.android.safetymapd
Version            26.31.0 (versionCode 2914950), minSdk 29, targetSdk 35, compileSdk
    36
Base APK size      104.8 MB (109,867,729 bytes)
Base APK SHA-256   b7a4e58e3e26dbd2d983cbc85c1f2853cf69e664453e6ab68f44878a294c7b14
Bundle SHA-256     fe16f642258e51c6e367cf290a7d7bbeaab732c401774fe5ae9df296616db3c8
Bundle             APKMirror .apkm release id 15533562
Audit device       none, the app was not installed
Acquisition        APKMirror, checked against the Google Play listing, 2026-08-23
```

```
google_api_key           AIzaSyBnUX4_tM-D5bW3aPF3ysEyxU-pgt2hWtk
google_app_id            1:316780013370:android:0ac587c694541924
gcm_defaultSenderId      316780013370
project_id               life360.com:l360safetycenter
firebase_database_url    https://life360-com-l360safetycenter.firebaseio.com
geo API_KEY              AIzaSyDJagPqPY8GrGF-enk_JChbGrxqeCLwP6s
dex key                  AIzaSyAYoKdlkfrse-Jdj15fc_FI0bht0mX_YBs
dex key                  AIzaSyBzmLWygDURw9zF3siSB_a5px5jsec4hLs
dex key                  AIzaSyDVsc4mFJOXNAFkx46vQCNkv-DZMHEjsdU
```

```
https://api.arity.com   https://api-staging.arity.com   https://tracking.arity.com
    https://tracking-staging.arity.com
https://api.sentiance.com   https://prod.uidapi.com   https://prod.euid.eu
api.eu.amplitude.com   regionconfig.eu.amplitude.com
dashboard.plaid.com   production.plaid.com   sandbox.plaid.com   analytics.plaid.com
withpersona.com   webrtc-consumer.withpersona.com   inquiry-fallback.withpersona.com
Contacts: privacy@life360.com, support.life360.com (help center), legal@life360.com (
    operator reply)
Representative: Osano International Compliance Services Limited, ATTN 4XK3, 3 Dublin
    Landings, North Wall Quay, Dublin 1, D01C4E0
```

```
C1  res/values/strings.xml (privacy_choices_*), Play Data Safety card
C2  AndroidManifest.xml (InitializationProvider, Sentiance receiver), classes dex
    strings, native library
H1  classes dex (com.bytedance.sdk.openadsdk, com.mbridge.msdk)
H2  classes dex strings (prod.uidapi.com, prod.euid.eu)
H3  AndroidManifest.xml (Plaid and Persona components), classes dex strings, res/
    values/strings.xml (dba_*)
H4  AndroidManifest.xml (DriverBehaviorReceiver, SleepClassifyReceiver), lib/arm64-v8a
    /libtensorflowlite_jni.so
M1  res/values/strings.xml, AndroidManifest.xml, classes dex strings
M2  res/xml/network_security_config.xml
```

Reproduction: obtain com.life360.android.safetymapd 26.31.0 (2914950), check the SHA-

256 value above, decode manifest and resources with apktool without source decode, extract the 8 classes dex files and search their strings, and read the Data Safety card of the Play listing. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF LIFE360-2026-R1 at 12:19 UTC to privacy@life360.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Three points, three questions, embargo date 21 November 2026.

2026-09-11 Reply from legal@life360.com at 19:05 UTC with pointers to the privacy policy and a statement on impact assessments.

2026-09-11 Answer from RFI-IRFOS at 19:23 UTC. Three questions restated, reply requested by 25 September 2026.

2026-09-29 Reply from legal@life360.com at 16:23 UTC. An Art. 27 representative is named, and questions 2 and 3 are described as answered.

2026-09-29 Answer from RFI-IRFOS at 17:55 UTC. Question 1 credited and closed, questions 2 and 3 restated as open.

2026-11-15 Supplementary notice from RFI-IRFOS at 14:02 UTC to legal@life360.com and privacy@life360.com, six days before publication: eight findings stated for the first time (C1 and C2 High, H1 to H4 Medium, M1 Medium, M2 Low), the contact address point withdrawn, the representative point closed, questions 2 and 3 restated.

2026-11-15 Automated confirmation of the privacy request from privacy@life360.com at 14:02 UTC. No substantive message and no delivery failure followed through 21 November 2026.

2026-11-21 Embargo date, 90 days after delivery of the notice of 23 August 2026.

What Was Done Well

The manifest sets usesCleartextTraffic to false, deliberately. allowBackup is set to false. A working age gate for children under 13 asks a parent or legal guardian to agree. The operator states that it does not sell or share information for targeted ads if it knows a member is under 18, in the standard and in the GDPR variants. A data subject rights flow for access and deletion exists for California. The app declares isMonitoringTool as child_monitoring, which is the honest declaration for a monitoring tool and the opposite of a disguised app. Sentry automatic start is switched off. The permissions for camera, location, microphone, nearby devices, notifications, phone, photos and physical activity are documented by the operator as optional, and the app works without them. The operator answered twice, named an Art. 27 representative with addresses, and said that impact assessments exist.

Residual Risk & Recommendations

Open at the date of publication: all eight findings. The operator has answered one of three questions. Whether the toggle of C1 defaults to off for accounts in the Union, and whether the Arity initializer samples at start, are the two points that would settle the largest findings. This report describes version 26.31.0 and the privacy policy as read for the analysis. A later APK or policy revision is not covered.

Recommendations in order of effect. First, move the sharing for third parties' own commercial use to opt-in consent and state the default for accounts in the Union (C1). Second, start Arity and Sentiance only after a consent decision (C2). Third, say whether the identity linkage of UID2 and EUID is active (H2) and which advertising networks run in the Union (H1). Fourth, state the basis and the transfer mechanism for Plaid and Persona (H3). Fifth, list the derived states and their retention (H4). Sixth, restrict the Google keys and consider pinning (M1, M2).

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 RFI-IRFOS research focus institute · ZVR 1015608684 ·

GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. Root level code analysis of the published application only. CVSS values are CVSS v4.0 Base (CVSS-B) and model technical exposure, so transparency findings fit the scale only approximately. Labels above the computed band carry a blast-radius escalation statement in the finding. Final report, published 21 November 2026. REF LIFE360-2026-R1.