Security & Privacy Disclosure, Final Report

Personal Safety (com.google.android.apps.safetyhub)

An emergency app by Google that creates a Google Contact about a named emergency contact, can pull location from every device on an account, and gives no retention period for emergency data, with no human reply from the operator.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 21 NOVEMBER 2026. NO HUMAN REPLY FROM THE OPERATOR, ONLY AUTOMATED REPLIES, THREE QUESTIONS OPEN.

Target	Google LLC, Personal Safety (Android app)
Version Audited	2026.08.06.960186296.0-release_gms / versionCode 100886377 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	7: 6 Medium, 1 Low
Status	NO HUMAN REPLY AS OF 21 NOVEMBER 2026. Automated replies of 23 August 2026 only, three questions open.
SHA-256 (base APK)	`1dbf57ea1db468dbf60668f21ad8e674817e7267250902c1b5f3bbbac393df48`

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: A Google API key and a legacy Firebase Realtime Database URL ship in every copy of an emergency app that depends on push messages 7

6.2 H1: The Firebase initialization provider creates an installation identifier at process start, before any screen and before the device is unlocked 8

6.3 H2: Starting Safety Check or Emergency Sharing can pull location from every device signed in to the same Google Account, and the notice sits in a settings flow 9

6.4 H3: Naming an emergency contact who is not in the user's Contacts creates a new Google Contact about that person before they answer the SMS invitation 10

6.5 M1: No retention period for emergency session data is stated anywhere in the package, and the location sharing backend is shared with Google Maps 11

6.6 M2: Emergency recording of up to 45 minutes of camera and microphone shares a download link with the emergency contacts by default, and it captures bystanders 12

6.7 M3: Three components that handle emergency information are exported without a permission in the manifest 13

7 Impact Analysis 14

8 The Complete Chain 14

9 Child Protection 15

10 Data Protection: Article by Article 15

11 Platform Accountability & DSA 16

12 Regulatory & Legal Landscape 16

13 Indicators of Compromise & Reproducible Evidence 17

14 Disclosure Timeline & Outcome 18

15 What Was Done Well 18

16 Residual Risk & Recommendations 19

Executive Summary

Personal Safety is the emergency app of Google LLC in Mountain View. It offers Emergency SOS, Emergency Sharing, Safety Check, car crash detection on Pixel devices, a medical ID and crisis alerts. The Play listing shows the content rating PEGI 3 with the descriptors Users Interact and Shares Location, a rating of 3.8 stars and 250K reviews. The app supports children who are under Google Family Link supervision. On 23 August 2026 RFI-IRFOS sent a notice with REF GOOGLEPERSONALSAFETY-2026-R1 to security@google.com and press@google.com, with the Austrian Datenschutzbehörde, the European Data Protection Supervisor and the Irish Data Protection Commission in copy.

A root level code analysis of version 2026.08.06 shows seven points. A Google API key and a legacy Firebase Realtime Database URL ship in the package of an app that depends on push messages for emergencies (C1). The Firebase initialization provider creates an installation identifier before any screen and before the first unlock (H1). Starting Safety Check or Emergency Sharing can pull location from every device on the same Google Account (H2). Naming an emergency contact who is not in the user's Contacts creates a new Google Contact about that person (H3). No retention period for emergency session data is stated (M1). Emergency recording of up to 45 minutes shares a download link with the emergency contacts by default (M2). Three exported components handle emergency information without a manifest permission (M3).

A reassessment by CVSS v4.0 band puts six findings at Medium and one at Low. The notice called C1 Critical and called H1 to H3 High. All four move to Medium, and M3, which was not in the notice, moves from Medium to Low. Each change is stated in the open items with its reason. No finding keeps a High or Critical label, because the package shows the presence of each mechanism and does not show a transmission, an exploit or a failure. The binary is also clean in the places where this programme often finds problems, with no advertising SDK, no session replay, no analytics suite and no background location permission.

Google answered with an automated message on 23 August 2026. The security-noreply address sent its standard text that points to the Bug Hunters site. The Irish Data Protection Commission, which was in copy, replied on the same day with a notice that its contact channel does not take queries under the EU AI Act. No person at Google has answered the three questions. A follow-up went out on 12 September 2026, a reminder on 17 October 2026 and a final notice on 15 November 2026, and none of them drew a reply by 21 November 2026.

Scope: Root level code analysis of the Personal Safety build 2026.08.06.960186296.0-release_gms (versionCode 100886377), obtained as base APK, 24,407,406 bytes, from the XAPK bundle of 24,649,970 bytes on the APKCombo mirror. The package identity and the developer name were checked against the live Google Play listing before download. Work done: full apktool decode with baksmali of 17,316 classes, manifest and resource review, string search over the resources and all classes, and a search for every URL in the package. The audit device was not reachable, so the app was not installed and no runtime test was done. The XAPK on the mirror carries the date 2026-08-18 and the live listing showed Updated on Aug 20, 2026, so the analysed build can lag the live one by one release. That lag is disclosed here and is not presented as a match with the live build. Out of scope: any call of the keys, of the database or of the components, the Family Link app, the Pixel car crash detection and a read of the live privacy policy.

ID	Severity	Title
C1	MEDIUM	A Google API key and a legacy Firebase Realtime Database URL ship in every copy of an emergency app that depends on push messages
H1	MEDIUM	The Firebase initialization provider creates an installation identifier at process start, before any screen and before the device is unlocked
H2	MEDIUM	Starting Safety Check or Emergency Sharing can pull location from every device signed in to the same Google Account, and the notice sits in a settings flow
H3	MEDIUM	Naming an emergency contact who is not in the user's Contacts creates a new Google Contact about that person before they answer the SMS invitation
M1	MEDIUM	No retention period for emergency session data is stated anywhere in the package, and the location sharing backend is shared with Google Maps
M2	MEDIUM	Emergency recording of up to 45 minutes of camera and microphone shares a download link with the emergency contacts by default, and it captures bystanders
M3	LOW	Three components that handle emergency information are exported without a permission in the manifest

Finding Status at a Glance

ID	Disclosed	This report	State on 21 November 2026
C1	CRITICAL	MEDIUM	Notice point 1. Restrictions, quotas and database rules not tested.
H1	HIGH	MEDIUM	Notice point 4. Scope narrow, transmission at start not observed.
H2	HIGH	MEDIUM	Notice point 3. Notice card exists, placement at activation not determined.
H3	HIGH	MEDIUM	Notice point 2. Order of steps and fate after a decline not verified.
M1	Question 2 only	MEDIUM	Question 2 of the notice. Retention statement may exist outside the package.
M2	MEDIUM	MEDIUM	Notice point 5. Expiry credited. Number of days set by the server.
M3	Not in notice	LOW	Exploitability not traced.

The notice of 23 August 2026 numbered its points 1 to 5. Point 1 is C1, point 2 is H3, point 3 is H2, point 4 is H1 and point 5 is M2. M1 reached the operator as question 2 and as a sentence on retention, and it carried no rating. M3 was not in the notice. This report uses

the CVSS v4.0 band of each finding. A downgrade is made only where the evidence in the package does not carry the earlier label, and every downgrade is listed in the open items with its reason.

Subject & Operator Analysis

The operator of Personal Safety is Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043, USA. The app is a first party product and no separate developer entity needed to be identified. The Union establishment of Google for the purpose of the GDPR is understood to be Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, according to the general Google privacy policy. This was not confirmed for this app and is UNVERIFIED at the level of the app. Question 3 of the notice asks Google to say so.

The package holds no privacy policy of its own, no data protection officer address and no app specific contact. The only policy links are policies.google.com/privacy, policies.google.com/terms and policies.google.com/terms/location. The notice therefore went to security@google.com and press@google.com, the addresses at which a report to Google is received. The live Play listing, checked on 23 August 2026, shows the rating 3.8 stars from 250K reviews, PEGI 3, a documented data deletion request mechanism and a statement that an independent security review was done against a global security standard.

The minimum SDK is 32 and the target SDK is 36, so the app runs on current Android versions only.

Architecture & Data Flow

The app is native Android with 17,316 classes. The functions are Emergency SOS, Emergency Sharing, Safety Check, emergency recording, a medical ID, crisis alerts and a bridge to Wear OS. Continuous location during an incident runs in IncidentForegroundService, a foreground service of the type location with a visible notification. The app does not request the permission ACCESS_BACKGROUND_LOCATION.

The data side has four parts. The first is push messages through Firebase Cloud Messaging and Firebase Installations (H1, C1). The second is location, which is shared with emergency contacts from one or several devices of the account (H2) through a location sharing backend that Google Maps also uses (M1). The third is the contact data of the people the user names, which becomes a Google Contact (H3). The fourth is emergency recording with a link for download (M2). Medical information is synced between paired devices and is described by the app as end to end encrypted, so that Google cannot access it.

The Firebase packages in the code are components, concurrent, datatransport, iid, installations, ktx, messaging and provider. No Analytics, Crashlytics, Performance or Remote Config package exists. The network security configuration enforces domain encryption and the manifest sets usesCleartextTraffic to false.

Engagement Summary

The notice REF GOOGLEPERSONALSAFETY-2026-R1 was sent on 23 August 2026 at 17:53 UTC from rfi.irfos@gmail.com to security@google.com and press@google.com, with dsb@dsb.gv.at, edps@edps.europa.eu and info@dataprotection.ie in copy. It carried five numbered points and three questions on the legal basis and information of the named contact, on the retention of emergency data and on the controller and the lead supervisory authority, and it set the embargo date of 21 November 2026. At 17:53 UTC the Irish Data Protection Commission (a supervisory authority and not the operator) answered with a notice that its channel does not take queries under the EU AI Act, and at 17:53 UTC the address security-noreply@google.com answered with its standard text that is not monitored by people and points to bughunters.google.com.

A follow-up on 12 September 2026 at 16:32 UTC restated the three questions and set the date 26 September 2026 for a reply. A reminder from security@rfi-irfos.com on 17 October 2026 at 19:09 UTC went to security@google.com and press@google.com without copies. A final notice from security@rfi-irfos.com followed on 15 November 2026 at 14:05 UTC to the same two addresses, six days before the embargo date. No further message arrived and no delivery failure was recorded by 21 November 2026. The notice did not use a bug bounty platform, and RFI-IRFOS does not route disclosures through them.

Findings

C1: A Google API key and a legacy Firebase Realtime Database URL ship in every copy of an emergency app that depends on push messages

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), disclosed as CRITICAL on 23 August 2026

The file res/values/strings.xml holds a Google API key twice, once as google_api_key and once as google_crash_reporting_api_key, with the Firebase project identifiers and a legacy Realtime Database URL. Anyone can read them from the package in under a minute. Google documents such keys as identifiers and not as secrets, so the exposure is availability, through quota exhaustion. The app delivers Safety Check timers, Emergency Sharing status and incident pushes through Firebase Cloud Messaging, which is why the point matters more here than in an ordinary app. RFI-IRFOS did not call the key and did not query the database. The key restrictions, the quotas and the database rules are not visible from the package and are UNVERIFIED.

```
[line 191]  default_web_client_id      624645263144-e963b3ehcu25bhmlf9963g30bfhf9tso.
    apps.googleusercontent.com
[line 471]  firebase_database_url     https://android-safety.firebaseio.com
[line 479]  gcm_defaultSenderId       624645263144
[line 499]  google_api_key            AIzaSyD-UoifT97CI5Zmq4UIa0qbAJydXpaWQcg
[line 500]  google_app_id             1:624645263144:android:10151a8275516624a4ca1d
[line 501]  google_crash_reporting_api_key  AIzaSyD-UoifT97CI5Zmq4UIa0qbAJydXpaWQcg
[line 951]  project_id                android-safety
```

The line numbers follow the findings file of the analysis. The same key value appears under two names. The package holds one key.

Impact: A quota exhaustion against the project could slow or stop functions that depend on it. Whether that reaches the delivery of emergency pushes depends on restrictions and quotas that the package does not show. The effect is on availability of a safety function. No personal data is exposed by the key itself.

Fix: Restrict the key by package name and signing certificate, review the quotas of the project, and review the rules of the Realtime Database or remove its URL if it is not used.

H1: The Firebase initialization provider creates an installation identifier at process start, before any screen and before the device is unlocked

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), disclosed as HIGH on 23 August 2026

The manifest declares com.google.firebase.provider.FirebaseInitProvider with init order 100 and directBootAware set to true. Android runs content providers during application creation, before any activity can show a screen, and a direct boot aware provider can run before the first unlock after a restart. The Firebase Installation ID and the Cloud Messaging registration are therefore set up before the user can see or answer any dialog. The decompiled code contains only the Firebase packages components, concurrent, datatransport, iid, installations, ktx, messaging and provider. No Analytics, Crashlytics, Performance or Remote Config package exists in the 17,316 classes. The identifier is the one that routes push messages, and a service that is strictly necessary for a requested function can fall under an exemption in Art. 5(3) of the ePrivacy Directive. Whether this applies to a start before the user has asked for any function is the open point.

```
<provider android:authorities="com.google.android.apps.safetyhub.fcmreceiver.
    firebaseinitprovider"
    android:directBootAware="true" android:exported="false" android:initOrder="100"
    android:name="com.google.firebase.provider.FirebaseInitProvider"/>
```

Impact: A persistent installation identifier exists on every device with the app, from the first start. The scope is narrow and the identifier serves push routing. Whether anything leaves the device at start was not observed.

Fix: State in the app and in the policy that the identifier is created at start and why, or defer registration until the first function that needs push messages is switched on.

H2: Starting Safety Check or Emergency Sharing can pull location from every device signed in to the same Google Account, and the notice sits in a settings flow

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B), disclosed as HIGH on 23 August 2026

Four strings in res/values/strings.xml describe a feature that the resource keys call MDR. When a user starts Safety Check or Emergency Sharing, location may be shared from all devices that are signed in to Personal Safety with the same Google Account. The stated reason is that Google can then choose the most accurate and most recent location for the emergency contacts. The app has a notice card with the title Sharing your location from multiple devices. The strings sit in an introduction and a notice card of a settings flow. Whether a user who starts Emergency Sharing for the first time has seen them at that point was not determined from the package.

```
[line 626] mdr_advantages_description:
"This helps your emergency contacts see your most accurate, real-time location during
    Emergency Sharing."

[line 628] mdr_introduction_description:
"When you start Safety Check or Emergency Sharing, your location may be shared from
    all devices signed in to the Personal Safety app using your Google Account."

[line 630] mdr_notice_card_description:
"When you start Safety Check or Emergency Sharing, you can now share your location
    from all devices signed in to the Personal Safety app using the same Google
    Account"

[line 634] mdr_reason_description:
"Making your location available from multiple devices at once helps Google determine
    which location is the most accurate and up-to-date to be shared with emergency
    contacts."
```

Impact: A person who expects that their phone shares its own position can have the position of a tablet or a second phone shared as well. The recipients are the emergency contacts that the user named. The feature serves the stated purpose, and the point is where the explanation appears and whether an impact assessment covers the wider footprint.

Fix: Show the multi-device explanation at the point where Safety Check or Emergency Sharing is first activated, and publish the data protection impact assessment for the feature.

H3: Naming an emergency contact who is not in the user's Contacts creates a new Google Contact about that person before they answer the SMS invitation

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B), disclosed as HIGH on 23 August 2026

The app's own warning string says that a new Google Contact will be created to add the named person, and that the contact will be available across Google services anywhere the user signs in. The text that tells the named person about the role is an SMS, and the app lets that person decline. The strings are shown to the user. They do not say when the record is created, and the findings file reads the text as creation at the moment the number is added, before the named person has seen or answered the SMS. The named person never installed the app and has given no consent to a record. The strings prove that the record is created and that the SMS and the decline exist. The order of the steps and the later fate of the record after a decline are UNVERIFIED.

```
[line 446] external_account_emergency_contact_warning_message:
"To add %1$s as an emergency contact, a new Google Contact will be created.
It will be available across Google services anywhere you sign in as %2$s."

[line 39] add_contact:
"A text message will be sent to %1$s to let them know they've been added as an
    emergency contact."

[line 1239] title_contact_declined:
"Your emergency contact declined"
```

Impact: The affected group is the people whom an app user names as emergency contact: relatives, partners and friends who did not install the app. A name and a phone number about them is stored in the Google account of the user. The record lives in the address book of the user, which is the user's own personal use. The open question is the basis and the information duty of the operator for the part of the processing that Google carries out.

Fix: Create the contact only after the named person accepts, or keep the number inside the emergency contact feature until then, and state in the SMS and in the policy what is stored about the named person.

M1: No retention period for emergency session data is stated anywhere in the package, and the location sharing backend is shared with Google Maps

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), raised as question 2 of the notice, not rated there

The package holds no privacy policy of its own for Personal Safety. The only policy links across the manifest, the resources and all 17,316 classes are the general Google pages policies.google.com/privacy, policies.google.com/terms and policies.google.com/terms/location. A search for retention, delete, stored for and days after in the context of incidents and location returned nothing. A migration string says that sharing with Safety Check and Emergency Sharing now uses the location permission of Personal Safety and no longer the one of Google Maps. The resource keys name the shared infrastructure LSR. The absence of a retention statement in the package is observed. That the retention is the same as for casual location sharing in Google Maps is an inference from the shared backend and is not shown.

```
https://policies.google.com/privacy
https://policies.google.com/terms
https://policies.google.com/terms/location
```

```
[line 574] lsr_consent_description_after_grace_period:
"Location sharing with Safety Check and Emergency Sharing now uses Personal Safety's
    location permission instead of Google Maps."

[line 583] lsr_onboarding_consent_description:
"Personal Safety uses location sharing with Safety Check and Emergency Sharing. This
    lets your emergency contacts see your real-time location during Emergency Sharing
    ."
```

Impact: A person in an emergency shares position, and possibly video, with named contacts. How long Google keeps that data, and whether the period differs from casual sharing, cannot be read from the app. A retention statement may exist in the general policy or on a web page that the package does not link.

Fix: Publish the retention period for Safety Check, Emergency Sharing and emergency recordings in the policy and link it from the app.

M2: Emergency recording of up to 45 minutes of camera and microphone shares a download link with the emergency contacts by default, and it captures bystanders

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), disclosed as MEDIUM on 23 August 2026

The strings say that the phone records for up to 45 minutes per video or until the user stops, and that after backup a link to download the video is automatically shared with the emergency contacts. The user can cancel the sharing when the recording ends. Sharing is therefore on by default, and the choice to stop comes later. The link note says that people with the link can see and download the video, so the access control is the possession of the URL. The link has a disclosed expiry, shown as a number of days that the server sets and that is not fixed in this build. A downloaded copy remains after the link expires. A recording of an emergency can show a partner, a child, a bystander or a stranger, and the situation can involve health, which brings Art. 9 into view.

```
[line 61]   auto_recording_feature_description_summary:
"Your phone records for up to 45 minutes per video or until you stop the recording.
    You can use your phone while it's still recording."

[line 320]  emergency_recording_auto_share_description:
"After backup, a link to download your video is automatically shared with your
    emergency contacts. You can choose to cancel sharing when recording ends."

[line 321]  emergency_recording_auto_share_title:  "Auto share"
[line 555]  link_expire_description:  "{days_left, plural, =1 {Link expires in # day}
    other {Link expires in # days}}"
[line 1102] share_link_description:  "Sharing via link"
[line 1103] share_link_notes:  "People with this link can see and download this video"
```

Impact: The people on the recording did not agree to it, and the contacts of the user receive a link to video and sound of them. The user chose the contacts and the feature, and the purpose is protection in an emergency. The weight is on the default and on the unauthenticated link.

Fix: Ask for a decision on sharing before the first recording, require sign-in for the link, and state the expiry period in the app.

M3: Three components that handle emergency information are exported without a permission in the manifest

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), first stated in this report

The manifest declares three exported components without an android:permission attribute. SafetyHubProvideAdditionalEmergencyInformationService answers the documented intent com.google.android.gms.els.REQUEST_EMERGENCY_INFO of the Emergency Location Service, a legitimate mechanism whose intended caller is the system. EmergencyInfoSuggestionStateProvider is a settings suggestion provider. ExportedEndpointService is the endpoint of the Wear bridge. Exported without a permission is necessary and not sufficient for misuse, because the code can check the caller inside the component. RFI-IRFOS did not trace the checks and did not send the intent from a test app, which is outside the scope of this report. Whether an unprivileged app can call the components and receive data is UNVERIFIED.

```
<service android:exported="true"
    android:name="com.google.android.apps.safetyhub.els.
    SafetyHubProvideAdditionalEmergencyInformationService">   (line 146)
<provider android:authorities="...suggestionstateprovider" android:exported="true"
    android:name="...platformsettings.EmergencyInfoSuggestionStateProvider">   (line
    328)
<service android:exported="true"
    android:name="com.google.android.apps.safetyhub.wearappbridge.listener.service.
    ExportedEndpointService"/>   (line 368)
```

Impact: If a caller check is missing, an app on the same device could ask for emergency information. The package does not show that this works and does not show what the answer holds.

Fix: Confirm that each component checks the caller, and add a signature permission where only the system or the Wear app should call.

Impact Analysis

The people affected are the users of an emergency app, a large group on Android 12L and later, and the people they name. The app is built for a moment in which a person is in danger. That raises the weight of every point: what the app collects, with whom it shares, for how long it keeps it, and whether it works.

The weight of the case sits at three points. A person who is named as an emergency contact becomes a record in a Google account before they answer (H3). Location can be shared from several devices at once, and the explanation sits in a settings flow (H2). Video and sound of an emergency go to the contacts of the user by link as a default, and nobody in the video chose that (M2). The key and the start up identifier are lower in weight. They do not expose personal data, and their effect would be on availability (C1) and on a narrow identifier (H1).

The analysis shows no failure of the emergency function and no leak. It shows design choices that need an answer.

The Complete Chain

Step 1, install: a user installs the app. Firebase initializes at process start and sets an installation identifier before any screen (H1).

Step 2, set up: the user names an emergency contact. If the person is not in the Contacts of the user, the app warns that a new Google Contact will be created, and an SMS goes to the person (H3).

Step 3, activation: the user starts Safety Check or Emergency Sharing. Location can be pulled from all devices on the account (H2) and goes through a backend that Google Maps shares (M1).

Step 4, recording: the phone records for up to 45 minutes. After backup, a link is shared with the emergency contacts by default, and people with the link can see and download the video (M2).

Step 5, availability: the push messages for these functions run through a project whose key is public in every copy of the app (C1).

The chain describes capability found in the package. Whether any step runs as described on a live device was not tested.

Child Protection

The group at the centre of this section is children and teenagers who use Personal Safety under Google Family Link supervision. The strings document a flow for them. A supervised user who wants to share location with emergency contacts is told to ask a parent to allow location access in Family Link. A supervised user who adds a contact that cannot be reached from the device is told to ask a parent to add the contact in Family Link. Both are real parental controls, and they limit H2 and H3 for supervised minors.

The open points are three. The Play rating PEGI 3 describes the content seen by the user and has no axis for the location, contact and recording pipeline behind it. The app can record video and sound for up to 45 minutes and share it by link (M2), and the package does not show whether a supervised account can do that. The age of digital consent in Austria is 14 under § 4 Abs. 4 DSG, and teenagers between 14 and 17 may use the app without Family Link supervision. For them, the pre-consent identifier (H1), the multi-device location sharing (H2) and the contact record (H3) apply as for adults.

The analysis found no data protection impact assessment for the supervised minor case in the package and does not assert that none exists. Family Link supervision is a parental consent mechanism, and the observation is raised as a question to the operator.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by H1, H2 and H3.

Article 5(1)(b), purpose limitation: engaged by H3, because a record that was created for the emergency contact function becomes a general Google Contact.

Article 5(1)(c), data minimisation: engaged by H2 for the wider footprint of the location pull.

Article 5(1)(e), storage limitation: engaged by M1.

Article 5(1)(f), integrity and confidentiality: engaged by M2 for the link that works for anyone who has it.

Article 6(1): engaged by H3 for the basis of the record about a person who is not a user.

Article 7(1): engaged by H1 for processing before any consent screen. The exemption of Art. 5(3) of the ePrivacy Directive for strictly necessary services is discussed in the finding.

Article 9: engaged by M2 where the recorded situation involves health. No processing of special categories is asserted beyond that.

Article 13 and Article 14: engaged by H2, M1 and H3. For the named contact, the data is not obtained from the person, so Art. 14 applies.

Article 25 and Article 32: engaged by C1, M2 and M3.

Article 35: engaged by H2 for the multi-device location pull.

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.

Google is the operator of the app and of the Google Play store that distributes it. The Data Safety card of the Play listing was not read for this report, so no statement is made on whether it matches the package. A reader of this report who wants the card compared with C1 to M3 can file a notice under Art. 16 of Regulation (EU) 2022/2065.

Regulatory & Legal Landscape

Google LLC offers Personal Safety to users in the Union through Google Play. Art. 3(1) of the GDPR applies if the processing takes place in the context of the activities of an establishment in the Union, and Art. 3(2) applies in any case. Google Ireland Limited in Dublin is understood to be the main establishment. If Google confirms that it is the controller for this app in the Union, the Irish Data Protection Commission is the lead supervisory authority under Art. 56, and the one-stop-shop mechanism applies. Without such a confirmation, the Austrian Datenschutzbehörde and the other authorities are competent under Art. 55 for users in their Member States. Question 3 of the notice puts this to Google. The Austrian Datenschutzbehörde (dsb@dsb.gv.at), the European Data Protection Supervisor (edps@edps.europa.eu) and the Irish Data Protection Commission (info@dataprotection.ie) received the notice in copy.

Infringements of Art. 5, 6, 7 and 9 and of Art. 12 to 22 fall under the upper fine tier of Art. 83(5). Infringements of Art. 25, 32 and 35 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 notice of 23 August 2026 also cited Art. 33(4) and said that the 72 hour clock was running. This report asserts no personal data breach. The package shows design choices and a public key and shows no incident.

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.google.android.apps.safetyhub
Version            2026.08.06.960186296.0-release_gms (versionCode 100886377), minSdk
    32, targetSdk 36
Base APK size      24,407,406 bytes
Base APK SHA-256   1dbf57ea1db468dbf60668f21ad8e674817e7267250902c1b5f3bbbac393df48
XAPK size          24,649,970 bytes
XAPK SHA-256       72c6156b35e61798824a17482200a7da287610104f1d3c3ecd1d231e294a9654
Classes            17,316 (apktool decode with baksmali)
Audit device       none reachable, the app was not installed
Acquisition        APKCombo mirror (apkcombo.com/de/personal-safety/com.google.android
    .apps.safetyhub/download/apk), mirror XAPK dated 2026-08-18, checked against the
    Google Play listing on 2026-08-23
```

```
default_web_client_id            624645263144-e963b3ehcu25bhmlf9963g30bfhf9tso.apps.
    googleusercontent.com
firebase_database_url           https://android-safety.firebaseio.com
gcm_defaultSenderId             624645263144
google_api_key                  AIzaSyD-UoifT97CI5Zmq4UIa0qbAJydXpaWQcg
google_app_id                   1:624645263144:android:10151a8275516624a4ca1d
google_crash_reporting_api_key  AIzaSyD-UoifT97CI5Zmq4UIa0qbAJydXpaWQcg
project_id                      android-safety
```

```
https://policies.google.com/privacy
https://policies.google.com/terms
https://policies.google.com/terms/location
Contacts: security@google.com, press@google.com (notice), security-noreply@google.com
    (automated reply), info@dataprotection.ie (automated reply)
Operator: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
Union establishment (UNVERIFIED for this app): Google Ireland Limited, Gordon House,
    Barrow Street, Dublin 4, Ireland
```

```
C1  res/values/strings.xml (lines 191, 471, 479, 499 to 501, 951)
H1  AndroidManifest.xml (line 285, FirebaseInitProvider)
H2  res/values/strings.xml (lines 626 to 634, mdr_*)
H3  res/values/strings.xml (lines 39, 446, 1239)
M1  full URL search over manifest, resources and all classes, res/values/strings.xml (
    lines 574, 583)
M2  res/values/strings.xml (lines 61, 320, 321, 555, 1102, 1103)
M3  AndroidManifest.xml (lines 146, 328, 368)
```

Reproduction: obtain com.google.android.apps.safetyhub 2026.08.06.960186296.0, check the SHA-256 value above, decode with apktool including baksmali, and read the files and lines named above. No device, account or network access is needed. Because the mirror can lag the live build, repeat the steps against the build that is live on the day of publication.

Disclosure Timeline & Outcome

2026-08-23 Notice REF GOOGLEPERSONALSAFETY-2026-R1 at 17:53 UTC to security@google.com and press@google.com, CC dsb@dsb.gv.at, edps@edps.europa.eu and info@dataprotection.ie. Five points, three questions, embargo date 21 November 2026.

2026-08-23 Reply from the supervisory authority info@dataprotection.ie (not the operator): the contact channel does not take queries under the EU AI Act.

2026-08-23 Automated reply from security-noreply@google.com at 17:53 UTC: not monitored by people, vulnerability reports to bughunters.google.com.

2026-09-12 Follow-up at 16:32 UTC. Three questions restated, reply requested by 26 September 2026.

2026-10-17 Reminder at 19:09 UTC from security@rfi-irfos.com to security@google.com and press@google.com. Three questions unchanged.

2026-11-15 14:05 UTC Final notice from security@rfi-irfos.com to security@google.com and press@google.com, six days before the embargo date, with the three questions open since 23 August 2026.

2026-11-21 No human reply and no delivery failure.

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

What Was Done Well

The app does not request ACCESS_BACKGROUND_LOCATION. Continuous location during an incident runs in a foreground service of the type location with a visible notification, which is data minimisation by design and not the pattern this programme usually finds.

Medical information that syncs between paired devices is described as end to end encrypted and not accessible to Google (line 644 of the resources).

The binary contains no advertising SDK, no session replay SDK, no SDK from a sanctioned jurisdiction and no attribution or analytics suite across 17,316 classes. Firebase is limited to Cloud Messaging and Installations.

Emergency video links carry a disclosed, user visible expiry. A named emergency contact receives an SMS and can decline the role, and the state Your emergency contact declined exists in the interface. The network security configuration enforces domain encryption, the manifest sets usesCleartextTraffic to false, and no custom trust anchor for user installed certificates is set. Children under Family Link supervision need a parent to allow location sharing and to add contacts that cannot be reached from the device. The live listing shows an independent security review and a documented data deletion request mechanism.

Residual Risk & Recommendations

Open on 21 November 2026: all seven findings and all three questions. The points that would settle the most are three. First, whether the Google Contact of H3 is created before the named person answers, and whether it is removed after a decline. Second, whether the multi-device notice of H2 is shown at the first activation. Third, whether a retention statement for emergency data exists outside the package (M1). RFI-IRFOS pulls the APK weekly and records any silent change in the public record without resetting the embargo.

Recommendations in order of effect. First, create the Google Contact only after the named person accepts, and tell that person what is stored (H3). Second, show the multi-device explanation at activation and publish the impact assessment (H2). Third, publish the retention period for emergency session data and recordings (M1). Fourth, ask for a sharing decision before the first emergency recording and require sign-in for the link (M2). Fifth, restrict the key and review the rules of the database (C1), state the identifier at start (H1) and confirm the caller checks of the exported components (M3).

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 GOOGLEPERSONALSAFETY-2026-R1.