Security & Privacy Disclosure, Final Report

Findmykids: GPS Locator for Kids (org.findmykids.app)

A child-location app with a detailed engineering dialogue, six verified fixes in 2.13.10 and nine points that the operator declared closed on 16 November 2026 without verification by RFI-IRFOS.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED, EMBARGO DATE 20 NOVEMBER 2026, OPERATOR REPLIED 16 NOVEMBER 2026

Target	LETEM LTD, Lakatameia, Nicosia, Cyprus
Version Audited	2.11.99-google / 2011991 (2026-08-22), checked 2.13.10 / 2013101 (2026-11-11). Version 2.13.15 (build 2013151) announced 2026-11-16, not checked
EU Representative	Alexej Sokolow, Postfach 71 01 31, 28761 Bremen, Germany
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	8: 1 Critical, 3 High, 3 Medium, 1 Low, plus 1 observation
Status	Substantive correspondence, six fixes verified, nine points declared closed by the operator on 16 November 2026, not verified by RFI-IRFOS
SHA-256 (base APK)	`466f1607e67fba2d5b05267d5cb0a4c033ebd094083b7c92cb30593efb510d26`

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 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Engagement Summary 7

6 Findings 8

6.1 C1: Firebase components start before device unlock and before any consent screen, no consent management platform in the binary, on a child-location app 8

6.2 C2: Russian Trusted Root CA in the app-wide trust anchor, legacy Russian carrier and sister-brand endpoints, a Russian hosting provider named in the policy 10

6.3 C3: Google Play Data Safety label said No data shared with third parties while the Privacy Policy named eight recipients 12

6.4 H1: Sound Around live microphone feature: bystander audio without notice, legal basis unresolved, RongCloud scope narrowed by the company's statement 13

6.5 H2: Accessibility service with system-wide window content retrieval on the child's device 15

6.6 H3: Firebase, AdMob and Facebook values hardcoded in the distributed binary 16

6.7 M1: Privacy Policy cites the EU-US Privacy Shield as a transfer safeguard . . . 17

6.8 M2: Cleartext HTTP permitted for one named MegaFon billing subdomain . . . 18

6.9 O1: Statements and consent methods shown to users: Stored on Russian servers, COPPA certified, ISO 27001, email plus 19

7 Impact Analysis 20

8 The Complete Chain 20

9 Data Protection: Article by Article 21

10 Consumer Protection & Platform Disclosures 22

11 Regulatory & Legal Landscape 22

12 Indicators of Compromise & Reproducible Evidence 23

13 Disclosure Timeline & Outcome 24

14 Operator Response of 16 November 2026 25

15 What Findmykids Got Right 26

16 Residual Risk & Recommendations 26

Executive Summary

Findmykids is a parent-facing child-location and device-monitoring app with 50M+ installs, rated PEGI 3, operated by LETEM LTD in Nicosia, Cyprus. One APK carries both the parent dashboard and the monitoring agent that runs on the child's phone: a Device Admin receiver, an Accessibility Service, a call screening service and a foreground microphone service. The app is not covert. It has a visible icon, a notice to the child and a described parental consent flow. On 22 August 2026 RFI-IRFOS disclosed three Critical, three High and two Medium findings from a root level code analysis of version 2.11.99 under REF FINDMYKIDS-2026-R1.

This is one of the few cases in the programme with a full engineering dialogue. Findmykids answered on 3 September 2026 with a named contact, and on 16 September 2026 with a class by class description of its Sound Around audio path, a fix plan for Firebase and a DPIA claim. On 11 November 2026 it wrote a final response and stated that all measures are shipped in version 2.13.10 (build 2013101). We pulled that build the same day and verified six items as closed: the Russian Trusted Root CA is gone, no Selectel, selcdn or MegaFon host remains, the AdMob key is gone, FcmListenerService is not exported, FCM auto-initialisation and Firebase Analytics collection are off with no direct-boot aware Firebase component, and the Privacy Policy no longer names Selectel or Russia.

Nine points were open after our verification. On 15 November 2026 we wrote again and repeated that the publication date stays 20 November 2026. On 16 November 2026 Findmykids answered each of the nine points and declared each one closed on the basis of the information it provided. These are statements by the operator, not verified by RFI-IRFOS. The operator stated that Crashlytics collection starts only after consent and that the change is in version 2.13.15 (build 2013151), submitted to Google Play on 16 November 2026 and live within two days. We did not pull that version, so the live state is not verified. It declined to show key restrictions, quota limits and the mapping file, sent two screenshots of the Realtime Database console and a functional description of the Sound Around audio path, and holds to contractual necessity as the legal basis. An internal legitimate interest assessment dated 16 November 2026 was attached and states that it does not change that reliance. The point by point record is in the section on the operator response.

We reassessed four disclosed ratings downward after the company's statements and the verified fixes (C2, H3, M2) and its statement on the Data Safety label (C3). Both notices of 22 August 2026 went to privacy@findmykids.org and support@findmykids.org with the Austrian DSB and the EDPS in copy. This report is published after the embargo date of 20 November 2026 was reached and records the state of the correspondence on 21 November 2026. No message from either side followed the operator reply of 16 November 2026.

Scope: Root level code analysis of the Google Play release 2.11.99-google (versionCode 2011991): manifest, resources, network security configuration, accessibility configuration, apksigner output and the string pools of eight classes*.dex files. The Google Play Data Safety section and the Findmykids Privacy Policy were read on 22 August 2026. Version 2.13.10 (build 2013101) was pulled from Google Play on 11 November 2026 and compared by the same method. No account was created, no feature was exercised, no Findmykids or RongCloud server was called and no traffic was intercepted. Items the package cannot show are marked as such. The decoded working folders of this case do not hold the raw evidence, so quoted manifest and string values come from the findings file of 22 August 2026 and from the notices.

ID	Severity	Title
C1	CRITICAL	Firebase components start before device unlock and before any consent screen, no consent management platform in the binary, on a child-location app
C2	MEDIUM	Russian Trusted Root CA in the app-wide trust anchor, legacy Russian carrier and sister-brand endpoints, a Russian hosting provider named in the policy
C3	HIGH	Google Play Data Safety label said No data shared with third parties while the Privacy Policy named eight recipients
H1	HIGH	Sound Around live microphone feature: bystander audio without notice, legal basis unresolved, RongCloud scope narrowed by the company's statement
H2	HIGH	Accessibility service with system-wide window content retrieval on the child's device
H3	MEDIUM	Firebase, AdMob and Facebook values hardcoded in the distributed binary
M1	MEDIUM	Privacy Policy cites the EU-US Privacy Shield as a transfer safeguard
M2	LOW	Cleartext HTTP permitted for one named MegaFon billing subdomain
O1	INFO	Statements and consent methods shown to users: Stored on Russian servers, COPPA certified, ISO 27001, email plus

ID	Disclosed	This report	Status on 21 November 2026

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	CRITICAL	Messaging and analytics fix verified in 2.13.10. Crashlytics consent fix stated for 2.13.15, not verified.
C2	CRITICAL	MEDIUM	Root CA, Selectel, MegaFon host removed in 2.13.10. Signing identity unchanged, explained.
C3	CRITICAL	HIGH	Company states the label was corrected. Current label not re-read.
H1	HIGH	HIGH	Audio chain: mapping file declined, functional description supplied, not verified. Legal basis and RongCloud scope: operator declared closed, not verified.
H2	HIGH	HIGH	Company position recorded. No change reported.
H3	HIGH	MEDIUM	AdMob key removed. Firebase values remain. Operator declined restriction evidence, sent two Realtime Database screenshots.
M1	MEDIUM	MEDIUM	Policy version disputed. Operator declined to correct section 9.2.
M2	MEDIUM	LOW	Resolved in 2.13.10.
O1	Not in notice	INFO	Raised as questions on 11 November 2026. Operator answered on 16 November 2026, not verified.

Subject & Operator Analysis

The Privacy Policy names LETEM LTD, 1 Arch Makariou III Avenue, 1st Floor, Office 101, Lakatameia, Nicosia 2324, Cyprus, as the controller. The privacy contact is privacy@findmykids.org and support is support@findmykids.org. The EU representative under Article 27 is Alexej Sokolow, Postfach 71 01 31, 28761 Bremen, Germany. A US telephone number for privacy requests appears in the policy and is not used, because RFI-IRFOS corresponds in writing only.

LETEM LTD is established in an EU member state. If Nicosia is the place of central administration within the meaning of Article 4(16), the Commissioner for Personal Data Protection of Cyprus is the likely lead supervisory authority under Article 56. Findmykids stated on 11 November 2026 that the company is registered in Cyprus, has its office there and that all decisions concerning the product are taken at that office. Contact details of the Cyprus authority are UNVERIFIED. RFI-IRFOS copies the Austrian DSB on every notice.

Findmykids stated that it acquired the product, the code and the signing certificates from a Russian company. The signing certificate of the distributed app names CN=Nikolay Kuznetsov, L=Perm, with SHA-256 840b08c86d54e2f1da81e96c4b3e5d18e712921ad0e16257d9e6ea6817c24596. The linked child app Pingo (org.findmykids.child) is a separate package with its own report.

Architecture & Data Flow

One APK, org.findmykids.app, holds the parent interface and the child agent. The child-side components are ChildDeviceAdminReceiver (Device Admin, anti-uninstall), AppAccessibilityService, ChildCallScreeningService and the foreground microphone service soundaround.childcore.ListeningService. Firebase provides messaging, analytics, crash reporting and sessions (C1). Billing, offer pages and a shop in version 2.11.99 pointed to a Russian sister brand (C2). RongCloud RTC components serve the GPS watch and video call functions according to Findmykids and are part of the build every user receives (H1).

Findmykids states that user data is processed on servers in Germany at Hetzner and that Sound Around audio runs from the child device over an AAC encoder and a TLS socket to a host and port supplied by the listen command, without storage. These descriptions are the company’s statements. They are not confirmed from the package, because the build is shrunk and renamed.

The package contains the SDKs AppsFlyer, Five Corp Ad and RongCloud, and hardcoded Firebase, AdMob and Facebook identifiers (H3). No NotificationListenerService and no household graph mechanism were found. The parent and child relation is declared by design and is not inferred.

Engagement Summary

The notice REF FINDMYKIDS-2026-R1 was sent twice on 22 August 2026 to privacy@findmykids.org and support@findmykids.org, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. The first message left at 14:19 UTC and the second at 17:05 UTC with a different text and the same reference. Both name 20 November 2026 as the publication date. The second message additionally lists the storage bucket and the web client ID.

Findmykids answered on 3 September 2026 through Egor Peresada, with colleagues in copy, point by point and with fix dates before 10 November 2026. We acknowledged the answers on the same day and asked for the exact audio path and the Firebase mechanism. A second answer of 16 September 2026 named the path and the mechanism, claimed a DPIA and attached a microphone sensitivity act. Our reply of 16 September 2026 accepted the Firebase fix in principle and raised three open points. A follow-up on 17 October 2026 repeated them. A final response on 11 November 2026 stated that all measures are in version 2.13.10. Our verification message of 11 November 2026 lists six items closed and nine open points with a reply requested by 16 November 2026. Our message of 15 November 2026 repeated that the publication date remains 20 November 2026. The operator replied on 16 November 2026 in nine numbered points with four attachments.

Findings

C1: Firebase components start before device unlock and before any consent screen, no consent management platform in the binary, on a child-location app

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 CRITICAL on 22 August 2026, messaging and analytics fix verified in 2.13.10, Crashlytics open, rated CRITICAL by blast-radius escalation

In version 2.11.99 the manifest declares FirebaseMessagingService and ComponentDiscoveryService with directBootAware set to true. ComponentDiscoveryService registers Messaging, Analytics Connector, Crashlytics and Sessions. A string search of res/values/strings.xml and all eight classes*.dex files for onetrust, didomi, usercentrics, consentmanager and iabtcf returned no hit. The app shows an Accept all consent screen with one item marked optional, which is a real granularity attempt and cannot gate components that start before unlock. Findmykids described the fix on 16 September 2026 (FCM auto-initialisation off, Analytics collection off, no direct boot path, activation after the consent event). Our check of version 2.13.10 on 11 November 2026 confirmed that FCM auto-initialisation and Firebase Analytics collection are switched off in the manifest and that no Firebase component is direct-boot aware. The manifest of 2.13.10 holds no firebase_crashlytics_collection_enabled entry, and Findmykids describes Crashlytics as consent-gated while its Privacy Policy table lists it under legitimate interest. That point is open. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the monitored person is a child who cannot consent, the app has 50M+ installs on Google Play, and no consent management platform exists in the binary. The CVSS vector scores only the technical exposure of a telemetry start.

```
<service android:directBootAware="true" android:exported="false"
    android:name="com.google.firebase.messaging.FirebaseMessagingService">
    <intent-filter android:priority="-500">
        <action android:name="com.google.firebase.MESSAGING_EVENT"/>
    </intent-filter>
</service>
<service android:directBootAware="true" android:exported="false"
    android:name="com.google.firebase.components.ComponentDiscoveryService">
    <meta-data android:name="com.google.firebase.components:com.google.firebase.
    messaging.FirebaseMessagingRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:com.google.firebase.
    analytics.connector.internal.AnalyticsConnectorRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:com.google.firebase.
    crashlytics.CrashlyticsRegistrar" .../>
    <meta-data android:name="com.google.firebase.components:com.google.firebase.
    sessions.FirebaseSessionsRegistrar" .../>
    <!-- plus Installations, IID and DataTransport registrars -->
</service>
```

Findmykids described the change on 16 September 2026 as: firebase_messaging_auto_init_enabled false, firebase_analytics_collection_enabled false, directBootAware false or default, and FirebaseMessaging.getInstance().isAutoInitEnabled set to true after the documented consent event. Verified against 2.13.10 on 11 November 2026: auto-initialisation and Analytics

collection off, no direct-boot aware Firebase component. Not verified and open: Crashlytics collection control.

Impact: A parent who installs the app to see where their child is has Firebase services start for them before the phone is unlocked and before they are asked. After the update in 2.13.10 this holds for messaging and analytics no longer. Whether crash reports leave the phone before consent is the remaining question.

Fix: Add firebase_crashlytics_collection_enabled false to the manifest and enable collection only after the recorded consent event. State the legal basis for Crashlytics in one form across the Privacy Policy and the consent screen.

C2: Russian Trusted Root CA in the app-wide trust anchor, legacy Russian carrier and sister-brand endpoints, a Russian hosting provider named in the policy

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), disclosed as CRITICAL on 22 August 2026, reassessed after the explanation of 3 September and 11 November 2026 and removal verified in 2.13.10, remaining open points are the signing identity and the consent screen texts (O1)

Version 2.11.99 bundled russian_trusted_root_ca in the base-config of the network security configuration, which makes it a trust anchor for every TLS connection of the app and not for Russian domains only. The binary hardcoded production endpoints on gdemoideti.ru (offer, gifts, shop, billing, cdn-frontend, webmapwidget), a package org.findmykids.support.paywalls.megafon with direct carrier billing, and a cleartext exception for megafon.gdemoideti.ru. The signing certificate names CN=Nikolay Kuznetsov, L=Perm. The Privacy Policy read at that time named Selectel Ltd as one of three hosts. Findmykids explained on 3 September and 11 November 2026 that the product, the code and the signing certificates were acquired from a Russian company, that the Root CA and Selectel proxying path were an attempt to keep access for users in Russia, that it did not work and was removed, that gdemoideti and MegaFon are legacy artefacts, and that user data is processed in Germany at Hetzner. It states that the main decisions are taken at its office in Cyprus. Our check of 2.13.10 on 11 November 2026 confirmed that the Root CA is gone (the configuration trusts system certificates and DST Root CA X3, with no cleartext exception), that no reference to Selectel, selcdn or a MegaFon host remains in code or resources, that gdemoideti survives as two package names in the package visibility list, and that the Privacy Policy no longer names Selectel or Russia. The signing certificate is unchanged by its nature and Findmykids states it cannot be replaced. The report records the origin as an explained fact and does not assert Russian control. The score covers the Root CA exposure that existed in 2.11.99 and is now removed.

```
<base-config>
    <trust-anchors>
        <certificates src="system" />
        <certificates src="@raw/dst_root_ca_x3" />
        <certificates src="@raw/russian_trusted_root_ca" />
    </trust-anchors>
</base-config>
<domain-config cleartextTrafficPermitted="true">
    <domain includeSubdomains="false">megafon.gdemoideti.ru</domain>
</domain-config>
```

```
Signer #1 certificate DN: CN=Nikolay Kuznetsov, L=Perm
Signer #1 certificate SHA-256 digest: 840
    b08c86d54e2f1da81e96c4b3e5d18e712921ad0e16257d9e6ea6817c24596
```

```
classes6.dex: https://gdemoideti.onelink.me/BfYh/ulxbzdv1
classes6.dex: https://gdemoideti.ru/megafon/gde_moi_deti_plus.pdf
classes6.dex: https://gifts.gdemoideti.ru/super?utm_source=gmd_app_android&utm_medium=
    app&utm_content=bonus_page
classes6.dex: android_feature_megafon_before_register
classes7.dex: https://offer.gdemoideti.ru/ru/pingo-watch/
classes7.dex: https://offer.gdemoideti.ru/en/pingo-watch-global/
classes7.dex: https://cdn-frontend.gdemoideti.ru/static/card.png
classes7.dex: https://shop.gdemoideti.ru/catalog/detskie_gps_chasy/...
classes7.dex: https://webmapwidget.gdemoideti.ru
classes7.dex: org.findmykids.paywalls.common.container.navigation.UpgradeMegafon(
    Confirm)
classes8.dex: https://billing.gdemoideti.ru/
classes8.dex: /api/landing/megafon/upgrade
classes8.dex: isMegafonSubscriptionBlocked
classes8.dex: org.findmykids.support.paywalls.megafon.internal.{main,data,confirm}.*
```

Privacy Policy section 5.2 as read on 22 August 2026, verbatim: Such partners include: Selectel Ltd (https://selectel.ru/en/about/documents/), Hetzner Online GmbH, and Google Cloud Platform.

Impact: A parent had to rely on a child-location app whose network configuration trusted a foreign state root certificate for all connections. Whoever could present a certificate issued by that root on the network path could have read or altered traffic of the app. The change in 2.13.10 removes this possibility for current installs once updated.

Fix: Keep the configuration as in 2.13.10, remove the remaining gdemoideti package names from the package visibility list, and explain the signing certificate origin in the Privacy Policy.

C3: Google Play Data Safety label said No data shared with third parties while the Privacy Policy named eight recipients

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as CRITICAL on 22 August 2026, reassessed to HIGH after Findmykids stated the label was corrected, current label to be re-read, rated HIGH by blast-radius escalation

On 22 August 2026 the Data Safety section of the Google Play listing stated: No data shared with third parties. The developer says this app doesn't share user data with other companies or organizations. Section 5 of the Privacy Policy read at that time named Selectel Ltd, Hetzner Online GmbH and Google Cloud Platform (hosting), Intercom, Inc. (support), The Rocket Science Group LLC (Mailchimp) and eSputnik Inc. (email), Facebook Inc. (advertising and measurement) and UserX Analytics (BUMPIN L.L.C-FZ) (analytics). Findmykids stated on 3 September and 11 November 2026 that it changed the Data Safety form and no longer relies on the earlier statement. The current label was not re-read for this report. This is a transparency finding with no technical vector, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the label is what parents read before installing an app that tracks a child, the app has 50M+ installs, and the operator's own policy contradicted it. The score is zero because no technical vector exists.

```
No data shared with third parties
The developer says this app doesn't share user data with other companies or
    organizations.
```

The Privacy Policy section 5 recipients above are quoted from the policy as it stood on 22 August 2026. Reproduction needs no tool: open the store page and the policy side by side. Further SDKs in the binary were AppsFlyer (Lcom/appsflyer/*), Five Corp Ad (Lcom/five_corp/ad/*), RongCloud (see H1) and the AdMob and Facebook identifiers listed under H3.

Impact: Parents read the Data Safety card before installing an app that follows their child. A card that says nothing is shared gives them a wrong picture of who receives their family's location data.

Fix: Keep the Data Safety form aligned with the Privacy Policy section 5 list and with the SDKs in each release.

H1: Sound Around live microphone feature: bystander audio without notice, legal basis unresolved, RongCloud scope narrowed by the company's statement

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, RongCloud scope narrowed by company statement, audio path pending, legal basis open, rated HIGH by blast-radius escalation

Version 2.11.99 declares org.findmykids.soundaround.childcore.ListeningService with foregroundServiceType microphone, the permissions RECORD_AUDIO and FOREGROUND_SERVICE_MICROPHONE, and RongCloud RTC classes (RongRtcAudioRecord, AudioRecordCallbackObserver) with the hosts stats.cn.ronghub.com, nav.cn.ronghub.com and cloudcontrol.rongcloud.net in the same package. The Privacy Policy describes listening live for 20 seconds, a notice to the child and no storage of audio on any servers. On 3 September and 11 November 2026 Findmykids stated that RongCloud is used only for children's GPS watches and their video calls (less than 1% of users), and that Sound Around runs through SoundChildPushHandler, SoundStarter, ListeningService, ListeningEngine, AudioStreamingSession, AudioToolsProvider, Android AudioRecord, AudioEncoderRuntime, Android MediaCodec, DataSenderRuntime and a Java SSLSocket, with host and port supplied by the listen command. It states that a DPIA exists, that the legal basis is legitimate interest, that microphone sensitivity was reduced, that a pre-activation audible notification is a test in the United States and the United Kingdom, and that Sound Around is not available in Austria. Our check of 2.13.10 on 11 November 2026 could confirm ListeningService under its plain name only. The other stages do not appear as class names because the build is shrunk and renamed, so the chain is pending until the R8 mapping file for build 2013101 is provided. RongCloud components remain part of the build every user receives. Whether audio of an EU family ever reaches a RongCloud endpoint was not tested and is not asserted. The people captured by the feature besides the child, siblings, classmates and other adults, receive no notice and have no consent mechanism of their own, and the balancing test for this group requested on 16 September 2026 was not provided. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the people recorded are children and other bystanders who cannot consent, the feature turns a phone into a live microphone, and the app has 50M+ installs. The score is zero because the package shows no technical exposure of the audio to an attacker.

```
<service android:foregroundServiceType="mediaPlayback" android:name="org.findmykids.
    soundaround.parent.ListeningPlayerService"/>
<service android:exported="false" android:foregroundServiceType="microphone" android:
    name="org.findmykids.soundaround.childcore.ListeningService"/>
<service android:exported="false" android:name="org.findmykids.geo.core.presentation.
    service.ListeningService" android:process="@string/geo_process"/>

android.permission.RECORD_AUDIO
android.permission.FOREGROUND_SERVICE_MICROPHONE
android.permission.MODIFY_AUDIO_SETTINGS
```

```
classes.dex:  Lcn/rongcloud/rtc/api/RCRTCAudioMixer$Mode;
classes3.dex: Lcn/rongcloud/rtc/api/probe/RTCProbeConfig;  Lcn/rongcloud/rtc/signal/
    IMSignalWrapper$*;
classes5.dex: Lcn/rongcloud/rtc/core/audio/RongRtcAudioRecord;
classes5.dex: Lcn/rongcloud/rtc/recordcallback/AudioRecordCallbackObserver;
classes5.dex: https://stats.cn.ronghub.com
classes5.dex: nav.cn.ronghub.com
classes5.dex: http://cloudcontrol.rongcloud.net/v1/config
classes.dex:  meta-data android:name="rc.rtclib" android:value="cn.rongcloud.rtc.api.
    RCRTCEngine"
```

Privacy Policy section 2.2.3.2 as read on 22 August 2026, verbatim: Sound around the child's device per request of the parent: you as a parent can choose to listen live to your child's device's surroundings for 20 seconds. Listening and recording are allowed only for the users with the Findmykids app installed and connected with the child's profile. The child is notified that they may be recorded. The Company does not store sound around the device or audio data on any servers.

Impact: The feature turns a child's phone into a microphone for one parent. Everyone within earshot of that phone is recorded without being told, which includes other children at school. A parent who activates it acts on a real worry, and the other people in the room never agreed to it.

Fix: Name the legal basis for the third-party audio in one form across the Privacy Policy, the DPIA and the correspondence, provide the balancing test, send the R8 mapping file for build 2013101, confirm that no RongCloud component starts for users without a watch, and publish the criteria and date for the pre-activation notification.

H2: Accessibility service with system-wide window content retrieval on the child’s device

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, necessity position of Findmykids recorded, open, rated HIGH by blast-radius escalation

The manifest declares org.findmykids.appblocksuperparentchild.AppAccessibilityService with BIND_ACCESSIBILITY_SERVICE. Its configuration sets canRetrieveWindowContent true, accessibilityEventTypes typeAllMask and the flags flagIncludeNotImportantViews, flagReportViewIds, flagRequestEnhancedWebAccessibility and flagRetrieveInteractiveWindows. Detecting the foreground app for a time limit needs only the window state change event. Findmykids stated on 3 September and 11 November 2026 that the screen content, down to text on the screen, is necessary for parental control, that it is not stored, and that it is read only where needed, for example when the child opens Settings or a browser. The package shows the configured capability. Whether content is read beyond that purpose was not tested and is not asserted. The correspondence leaves the data minimisation question with the company’s own account. This item was not part of the open points of 11 November 2026. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the service runs on a minor’s phone, can read the content of every other app, and the app has 50M+ installs. The score is zero because the package shows capability and no demonstrated misuse.

```
<service android:exported="false" android:name="org.findmykids.
    appblocksuperparentchild.AppAccessibilityService"
         android:permission="android.permission.BIND_ACCESSIBILITY_SERVICE">
    <intent-filter><action android:name="android.accessibilityservice.
    AccessibilityService"/></intent-filter>
    <meta-data android:name="android.accessibilityservice" android:resource="@xml/
    accessibility_service_config"/>
</service>
```

```
<accessibility-service
    android:description="@string/
    app_block_super_parent_child_block_accessibility_service_description"
    android:accessibilityEventTypes="typeAllMask"
    android:accessibilityFlags="flagDefault|flagIncludeNotImportantViews|
    flagReportViewIds|flagRequestEnhancedWebAccessibility|
    flagRetrieveInteractiveWindows"
    android:canRetrieveWindowContent="true"
    android:notificationTimeout="100" />
```

Impact: Parental control on a child’s phone needs this kind of access to block content. The same access can in principle read the text of every app on that phone. The child, usually a minor, carries this on a device that is also used for private conversations.

Fix: Document which events and which window contents the service reads, restrict the event types to those needed for blocking, and state the retention of any content that leaves the device.

H3: Firebase, AdMob and Facebook values hardcoded in the distributed binary

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 HIGH on 22 August 2026, reassessed to MEDIUM because a Firebase key is not a secret by design, AdMob key removed, key restrictions open

res/values/strings.xml of version 2.11.99 carries the values below in plain text. A Firebase key is not a secret by Google design, so the demonstrated exposure is availability through quota and billing exhaustion, and the open question is whether the key restrictions, App Check and the Security Rules are set correctly. Findmykids stated on 3 September 2026 that the weak restrictions were noticed and will be tightened by package ID and SHA-1, and on 11 November 2026 that the keys are restricted to the required APIs and to its authorised products. Our check of 2.13.10 confirmed that the AdMob application key is gone. The Firebase API key, the sender ID, the app ID and the Realtime Database URL named in the first notice remain in the build. Realtime Database classes are absent from 2.13.10, so use of the database is not claimed. Whether the google_geo_api_key, the storage bucket and the web client ID remain in 2.13.10 was not stated in the message of 11 November 2026 and is open. No call was made against any project. Screenshots of the key restrictions, quota limits, App Check status and the Realtime Database API status were requested.

```
<string name="google_api_key">AIzaSyDZp3fcu7xmJyoAHTFhQR5t47-W-4HNpOY</string>
<string name="google_crash_reporting_api_key">AIzaSyDZp3fcu7xmJyoAHTFhQR5t47-W-4HNpOY
    </string>
<string name="google_app_id">1:339625562515:android:191231a17fd56a57</string>
<string name="project_id">where-is-my-children</string>
<string name="google_storage_bucket">where-is-my-children.appspot.com</string>
<string name="gcm_defaultSenderId">339625562515</string>
<string name="default_web_client_id">339625562515-qeuh3npui511kmuff36bu67jg098d5gf.
    apps.googleusercontent.com</string>
<string name="google_ads_app_id">ca-app-pub-1647054784468373~7788327316</string>
<string name="google_geo_api_key">AIzaSyAjecI_SkPNkmljyMk6ZkH8uc21ARFTy7U</string>
<string name="facebook_app_id">820328364255380</string>
<string name="facebook_client_id">92369e3d32f5d379c4662cd36d38c9a2</string>
```

The Firebase project name where-is-my-children is the legacy name of the product and is still the live project identifier. Every value is extractable with apktool from any copy of the app.

Impact: If the project were rate-limited by quota exhaustion, push messages and location features that families rely on would be affected. The key stays in every installed copy until an app update replaces it.

Fix: Restrict each key by package name, signing certificate and API scope, enforce App Check, and confirm deny-by-default Security Rules. Rotate the google_geo_api_key if it is unrestricted.

M1: Privacy Policy cites the EU-US Privacy Shield as a transfer safeguard

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as MEDIUM on 22 August 2026, policy version disputed, current wording to be re-read, open

The first notice quoted section 9.2 of a Privacy Policy with the effective date 11 March 2022, which names the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks as a transfer safeguard. The Court of Justice of the European Union invalidated the Privacy Shield on 16 July 2020 (Case C-311/18, Schrems II). Findmykids stated on 3 September 2026 that this was an outdated version redirected to a new one and that the old version was removed. The effective date of March 2022 therefore applied to the older document, and this report does not rely on it. Our message of 11 November 2026, written after reading the current policy at findmykids.org/documents?docId=2&sectionId=2, states that its section 9.2 still relies on the EU-U.S. Privacy Shield. The policy text itself is not stored in the case folder, so the wording of the current section 9.2 is to be read again before publication. The question whether DPIA section 3.6, which states that no cross-border transfer takes place, and section 9.2 will be corrected is open. This is a legal finding with no technical vector.

```
...we make use of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, European
    Commission-approved standard contractual data protection clauses, or other
    appropriate legal mechanisms to safeguard the transfer.
```

Impact: A parent who reads the transfer section is told about a safeguard that no longer exists. The text gives a false sense of how transfers are protected.

Fix: Replace the Privacy Shield reference with the actual current mechanism, for example the EU-U.S. Data Privacy Framework or Standard Contractual Clauses, and align DPIA section 3.6.

M2: Cleartext HTTP permitted for one named MegaFon billing subdomain

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), disclosed as MEDIUM on 22 August 2026, reassessed to the single-host band, resolved in 2.13.10

Version 2.11.99 set cleartextTrafficPermitted true for the single domain megafon.gdemoideti.ru (includeSubdomains false) in the network security configuration. The first notice stated precisely that this is a narrow carve-out and not an app-wide exposure. Our check of 2.13.10 on 11 November 2026 confirmed that the configuration trusts system certificates and DST Root CA X3 with no cleartext exception. The finding is resolved in 2.13.10 (build 2013101).

```
<domain-config cleartextTrafficPermitted="true">
    <domain includeSubdomains="false">megafon.gdemoideti.ru</domain>
</domain-config>
```

Impact: Only users of the MegaFon billing path in the older versions were affected. The exposure was a single host and is gone in the current version.

Fix: None for this item. Keep cleartext denied by default.

O1: Statements and consent methods shown to users: Stored on Russian servers, COPPA certified, ISO 27001, email plus

INFO, no CVSS v4.0 score assigned, raised as questions on 11 November 2026, not rated

Our message of 11 November 2026 reports that the build of 2.13.10 contains consent screen texts under the resource keys personalisation_license_feature_* with the wording Stored on Russian servers, We are COPPA certified, All data about you and your kid is anonymized and protected from being shared with third parties, and The app complies with the ISO 27001 standard. The same build offers Simple consent labelled as the email plus method and Full consent, whose text says Findmykids may collect, use and disclose the following child's data. The questions were whether the screen is shown, to whom and in which regions, which program and certificate stands behind COPPA certified, which certificate holder, issuer and scope stands behind ISO 27001, which consent method applies to which users, and whether children's personal information is disclosed to a third party. 16 CFR 312.5(b)(2)(viii) makes email plus available to an operator that does not disclose children's personal information. The wording is quoted from our message. The resource strings are not stored in the case folder. The observation is not rated. The operator answered on 16 November 2026 that the screen is a legacy screen that no user sees in any region and that the texts were removed, which is not verified by RFI-IRFOS.

```
personalisation_license_feature_*:
  Stored on Russian servers
  We are COPPA certified
  All data about you and your kid is anonymized and protected from being shared with
    third parties
  The app complies with the ISO 27001 standard

Simple consent (labelled email plus)
Full consent: Findmykids may collect, use and disclose the following child's data
```

Impact: A parent reading these lines is told about storage in Russia, a certification and an international standard. If they do not match the facts, the parent decides on wrong information.

Fix: Show only statements that the operator can document, name the certificate holder for each certification, and align the text with the stated processing in Germany.

Impact Analysis

The people affected are parents who use the app to see where their child is, and the children who carry it. A child is not the account holder and cannot consent for themselves. The feature set is broad: location, an anti-uninstall Device Admin, an accessibility service that can read the screen, and a live microphone.

In version 2.11.99 the largest structural exposures were the pre-consent start of Firebase (C1) and the Russian root certificate in the app-wide trust anchor (C2). Both are closed in 2.13.10 for messaging and analytics, and for the Root CA. The remaining weight sits on Sound Around (H1) because it records people who have no relationship with the operator, on Crashlytics (C1) and on the transparency of what the app tells parents (C3, M1, O1).

The demonstrated harm is a harm of transparency and default configuration. No access to location, accounts or audio was shown, and none was tried.

The Complete Chain

Step 1, store: a parent compares child trackers. The Data Safety card said no data is shared (C3).

Step 2, install and first launch: Firebase components start before unlock in the version of 22 August (C1). In 2.13.10 messaging and analytics are off until consent. Crash reporting is not shown to be gated in the version we checked. The operator states that version 2.13.15 gates it on consent.

Step 3, consent and linking: the parent accepts a consent screen with an optional item and a parental consent method (O1). The child app is linked to the child’s profile.

Step 4, operation: the child device sends location. The accessibility service reads screen content where the parental control needs it (H2).

Step 5, Sound Around: the parent triggers a live listening session of 20 seconds. The child gets a notice and bystanders get none (H1). The legal basis is stated two ways.

Step 6, the parent tries to learn how the data is protected: the policy cited a transfer safeguard that no longer exists (M1).

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C3, H1, M1 and O1.

Article 5(1)(c), data minimisation: engaged by H1 and H2.

Article 5(2), accountability: engaged by C1 (documented consent for Crashlytics) and H3 (burden of proof for key restrictions).

Article 6(1), lawful basis: engaged by C1 and H1. For Sound Around the Privacy Policy lists contractual necessity under Article 6(1)(b), DPIA section 3.1 names Article 6(1)(b) and the company's message names legitimate interest under Article 6(1)(f). The operator stated on 16 November 2026 that contractual necessity is the only legal basis and attached an internal legitimate interest assessment with a favourable result for the case that legitimate interest applied. That assessment states that it does not establish Article 6(1)(f) as the basis. Which basis applies is open for RFI-IRFOS.

Article 7(1), conditions for consent: engaged by C1.

Article 8, child consent: noted for O1, because the parental consent method is under question.

Article 9: engaged by H1 as a question for voice data that can reveal health related information. No finding of a special category processing is asserted.

Article 12(1) and Article 13(1)(e) and (f): engaged by C3, H1 and M1.

Article 25: engaged by H2 and H3.

Article 27: met. The Bremen representative is named and is credited below.

Article 28: not asserted. The company describes the Kids360 SDK in the Pingo case only.

Article 32(1)(a) and (b): engaged by C2, H3 and M2.

Article 35: engaged by H1. A DPIA exists according to the company. The version we read is dated 1 July 2023 and the file was created on 11 November 2026. The company states that the DPIA was approved on 1 July 2023 and signed. The file shows signature marks for the CTO and the DPO, with no date beside them, and the signature annotations carry modification stamps of 11 November 2026 (08:23 and 08:37 UTC). That does not show when the approval decision was taken. We first recorded both lines as blank after reading the text layer of the file. The operator asked on 16 November 2026 for a review of the document itself, and we corrected the record in this report on 17 November 2026. The operator adds that the file creation date reflects a copy made when it collected evidence. The balancing test for non-user third parties is not in it. The operator listed the DPIA sections that deal with bystanders and states that its reply of 16 November 2026 answers the point.

Articles 44 and 46: engaged by C2, H1 and M1. The company states that data stays in Germany. The question for watch users, the country of RongCloud and Jufeng processing and the transfer mechanism, is open. The operator states that watch calling uses RongCloud or Jufeng depending on the watch model and that the processing location is set by the watch manufacturer. It states that Sound Around is not routed through either.

ePrivacy Directive Article 5(3): engaged by C1.

Consumer Protection & Platform Disclosures

The Data Safety section of the Google Play listing stated No data shared with third parties on 22 August 2026. The Privacy Policy named eight recipients at that time (C3). Findmykids states that the form was changed. The current label was not re-read for this report.

The consent screen texts in the build, Stored on Russian servers, We are COPPA certified, All data about you and your kid is anonymized and protected from being shared with third parties and The app complies with the ISO 27001 standard, are statements to consumers that need a documentable basis (O1). The FTC guidance on children's privacy refers to FTC-approved safe harbor programs and does not provide for certification of apps by the FTC. ISO/IEC 27001 certifies an organisation's management system and the certificate holder, issuer and scope are the facts that make the statement checkable. The operator states that the screen carrying these texts is a legacy screen that no user sees in any region, that the texts were removed, and that one active consent screen covers the Privacy Policy and analytics. RFI-IRFOS has not verified this.

Regulatory & Legal Landscape

The framework applied is the GDPR and the ePrivacy Directive, together with the COPPA rule (16 CFR Part 312) where the app is offered to US families. The operator is established in Cyprus. The Cyprus Commissioner for Personal Data Protection is the likely lead authority if Nicosia is confirmed as the place of central administration. Any other supervisory authority may act for data subjects in its territory in the cases the GDPR allows.

The NISG 2026 applies from 1 October 2026 and no obligation under it, under NIS2 or under the AI Act is asserted for this operator. The disclosure follows ISO/IEC 29147 and Art. 17 StGG. The competent Austrian authority is the Österreichische Datenschutzbehörde (dsb@dsb.gv.at). The European Data Protection Supervisor (edps@edps.europa.eu) is in copy of the notice.

Findmykids states that Sound Around is not available in Austria. The listening classes are part of the package that Austrian users receive. Where the gate is enforced, in the client or on the server, was asked on 11 November 2026. The operator answered on 16 November 2026 that the restriction is enforced in the client, using the device location and the SIM card, and that the server does not reject a listen command on the basis of Austria alone. This is stated by the operator, not verified by RFI-IRFOS.

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            org.findmykids.app
Version audited    2.11.99-google (versionCode 2011991), analysed 2026-08-22
base APK SHA-256   466f1607e67fba2d5b05267d5cb0a4c033ebd094083b7c92cb30593efb510d26
XAPK SHA-256       5818eb04f44742f200514c54ef96e450ea58e0978dc260a9b6dd4e57cf275ee7
Signing cert SHA-256 840b08c86d54e2f1da81e96c4b3e5d18e712921ad0e16257d9e6ea6817c24596
Signer DN          CN=Nikolay Kuznetsov, L=Perm
minSdk / targetSdk 32 / 36

Version checked    2.13.10 (build 2013101), pulled 2026-11-11
base.apk SHA-256   f2133bc09d80957130f46cc34bf1d961bc65a7efcf0ced46f24bec8b3cf2d3a9
split_config.arm64_v8a.apk SHA-256  0936
    d4058526cd1c84ba6d1a1bf55f4473556ca85fdd6e479144c2fa00057d81
split_config.xxhdpi.apk SHA-256     05126313
    a4c71fe41cc0d9ea0796188177c71e83b9556ad7a52d3f88e4f5303c

Firebase project   where-is-my-children
Database URL       https://where-is-my-children.firebaseio.com (named in the message
    of 11 November 2026 and in the Pingo case for the same project, not in the
    findings file)
google_api_key     AIzaSyDZp3fcu7xmJyoAHTFhQR5t47-W-4HNpOY
google_geo_api_key AIzaSyAjecI_SkPNkmljyMk6ZkH8uc21ARFTy7U
google_app_id      1:339625562515:android:191231a17fd56a57
gcm_defaultSenderId 339625562515
Storage bucket     where-is-my-children.appspot.com
Web client ID      339625562515-qeuh3npui511kmuff36bu67jg098d5gf.apps.
    googleusercontent.com
AdMob app ID       ca-app-pub-1647054784468373~7788327316
Facebook app ID    820328364255380
Facebook client ID 92369e3d32f5d379c4662cd36d38c9a2
RongCloud hosts    stats.cn.ronghub.com, nav.cn.ronghub.com, cloudcontrol.rongcloud.
    net
Offer link         https://gdemoideti.onelink.me/BfYh/ulxbzdv1
```

```
C1  AndroidManifest.xml (FirebaseMessagingService, ComponentDiscoveryService), strings
    .xml and classes*.dex (consent platform search)
C2  res/xml/network_security_config.xml, apksigner output, classes6.dex to classes8.
    dex, Privacy Policy section 5.2
C3  Google Play Data Safety section (22 August 2026), Privacy Policy section 5
H1  AndroidManifest.xml (ListeningService), classes.dex, classes3.dex, classes5.dex (
    RongCloud), Privacy Policy section 2.2.3.2
H2  AndroidManifest.xml, res/xml/accessibility_service_config.xml
H3  res/values/strings.xml
M1  Privacy Policy section 9.2
M2  res/xml/network_security_config.xml
O1  resource keys personalisation_license_feature_* (as quoted in the message of 11
    November 2026)
```

Reproduction: obtain org.findmykids.app 2.11.99-google, check the SHA-256 above, decode

with apktool and run apksigner on the package. The same steps with 2.13.10 show the changes. No device, account or network access is needed. The raw decoded folders are not part of this case folder.

Disclosure Timeline & Outcome

2026-08-22 Notice REF FINDMYKIDS-2026-R1 at 14:19 UTC to privacy@findmykids.org and support@findmykids.org, CC DSB and EDPS. An automatic reply from the support desk followed within a minute and gave no reply on the findings. A second notice with the same reference and a fuller text left at 17:05 UTC in a separate thread and received no reply.

2026-09-03 Substantive reply from Egor Peresada, in seven points, with fix dates before 10 November 2026 and a designated contact. Our acknowledgement the same day asked for the exact audio path and the Firebase mechanism.

2026-09-16 Second reply: audio path named, Firebase fix described with a date of 11 November 2026, DPIA claimed, microphone sensitivity act attached. Our reply the same day raised three open points.

2026-10-17 Follow-up, 34 days before the embargo date, repeating the three points. An automatic reply from the support desk followed on 2026-10-18 and gave no reply on the findings.

2026-11-11 Final response of Findmykids: all measures in version 2.13.10 (build 2013101). Our verification message the same day: six items closed, nine points open, reply requested by 16 November 2026.

2026-11-15 Message from security@rfi-irfos.com at 14:07 UTC, five days before the embargo date, stating that the publication date remains 20 November 2026. An automatic reply from the support desk followed at 14:09 UTC and gave no reply on the findings.

2026-11-16 Reply from Egor Peresada at 16:26 UTC in nine numbered points, each declared closed by the operator. Version 2.13.15 (build 2013151) announced as submitted to Google Play that day. The operator declined screenshots of key restrictions and the R8 mapping file and attached Appendix A, an internal legitimate interest assessment dated 16 November 2026 and two screenshots of the Realtime Database console.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026.

2026-11-21 Publication of this report. No message from either side after 16 November 2026 at 16:26 UTC. The thread holds 13 messages: six from RFI-IRFOS, four human replies and three automatic replies from the operator.

Operator Response of 16 November 2026

Statements of the operator, reply of 16 November 2026 (Egor Peresada, 16:26 UTC, REF FIN DMYKIDS-2026-R1). Each point ends in the sentence ”We consider this point closed on the basis of the information provided above.” Everything below is stated by the operator and not verified by RFI-IRFOS unless a verification is named.

1. Crashlytics and consent. ”Crashlytics is handled in the same way as Firebase Analytics.” The change is in version 2.13.15 (build 2013151), submitted on 16 November 2026. We did not pull it. Status for RFI-IRFOS: open until the build is checked.

2. Firebase keys, App Check, Realtime Database. The operator declined to provide restriction and quota details as security-sensitive, states that additional restrictions were applied after our report, that Firebase App Check is not integrated and that Realtime Database is not used. Screenshot 1 shows the console of where-is-my-children.firebaseio.com with an Enable button, and screenshot 2 shows the rules read false and write false. We cannot confirm account, project or time from the images. Status: restrictions not evidenced, open.

3. Sound Around audio path. The mapping file was declined. Appendix A lists functional indicators (AudioRecord, MediaCodec, AAC at 32000 bit/s, SSLSocket, host and port supplied at session start) and states that the stream goes to LETEM LTD infrastructure in Falkenstein, Germany and not through RongCloud. We have not traced these indicators in a build. Status: pending.

4. RongCloud and GPS watches. RongCloud or Jufeng may be used depending on the watch model, the manufacturer determines the processing location, and Sound Around does not use them. The country and the transfer mechanism for watch users remain unnamed. Status: open.

5. Legal basis, DPIA, policy. The operator relies on Article 6(1)(b) only, states that the DPIA was approved on 1 July 2023 and signed, and asked us to review the document itself. It will not correct DPIA section 3.6 or Privacy Policy section 9.2 and explains that the policy says ”may” and describes a possibility. The attached assessment is dated 16 November 2026 and carries an internal status line that it is subject to technical and factual verification. Its overall outcome is favourable, and it states that it does not change the declared reliance on Article 6(1)(b). Status: open.

6. Microphone sensitivity. ”The sensitivity level was reduced from 5.5 to 1.75”, stated as present in 2.13.10 and shared with Pingo. The audible pre-activation notification ”remains under evaluation” with no fixed decision date. Status: value not verified at the build.

7. Austria region gate. Enforced on the client by device location and SIM card, with no server-side rejection. Status: recorded.

8. Consent screen texts. The screen is a legacy screen shown nowhere and the texts were removed. Status: not verified.

9. Parental consent. Email plus consent where no more than two parents are connected, full consent for a third user. The operator treats the COPPA question as outside the GDPR matters. Status: recorded.

What Findmykids Got Right

Findmykids answered with named, point by point engineering detail, which is rare in this field. It described its audio path class by class, described its Firebase fix in manifest terms, shipped the fixes in a version number and told us when. The child receives an on-device notice before a listening session. A COPPA email plus parental consent flow is described for the linked child app. A real Article 27 representative is named in Bremen. allowBackup is false and targetSdkVersion is 36. The AppsFlyer item on the consent screen is marked separately optional. The company names its hosting provider in the policy, and the policy states a commitment not to use data of children under 13 for advertising. The Root CA, the Selectel path, the MegaFon host and the AdMob key were removed in 2.13.10, and the cleartext exception is gone. On 16 November 2026 it answered all nine points in writing within the requested time and attached its own assessment and a functional description of the audio path.

Residual Risk & Recommendations

Not verified by RFI-IRFOS at the date of publication. The operator declared each point closed on 16 November 2026. The list follows our message of 11 November 2026 and the findings above: Crashlytics collection control (C1), Firebase key restrictions with App Check and the Realtime Database API status (H3), the R8 mapping file for the audio chain (H1), RongCloud initialisation for users without a watch and the country of processing for watch users (H1), the single legal basis for Sound Around and the balancing test for bystanders (H1), the build and value of the microphone sensitivity reduction (H1), the decision criteria and date for the pre-activation notification (H1), the location of the region gate (H1), the consent screen texts (O1) and the parental consent method (O1).

Recommendations: gate Crashlytics on the consent event, show restriction and App Check evidence for the Firebase keys, send the mapping file, name one legal basis for Sound Around and provide the balancing test, publish the decision criteria for the pre-activation notification, correct Privacy Policy section 9.2 and DPIA section 3.6, remove the gdemoideti package names, and document the claims on the consent screen.

This report is published after the embargo date. Statements are limited to the packages and public documents named above and to the company’s own written statements, which are recorded as statements and not as verified facts unless a verification is named.

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 Root level code analysis of the published application

plus public documents read from the public sites. No Findmykids or RongCloud servers, devices or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF FINDMYKIDS-2026-R1.