Security & Privacy Disclosure, Final Report

Pingo: Chat with Parents (org.findmykids.child)

The child side of a monitoring product, an acknowledged exported service now closed in 2.13.6, and eight 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	2.11.96-google / 2011960 (2026-08-22), checked 2.13.6 / 2013060 (2026-11-14). Version 2.13.7 (build 2013070) 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	7: 1 Critical, 1 High, 5 Medium, plus 1 observation
Status	Substantive correspondence, six fixes verified, eight points declared closed by the operator on 16 November 2026, not verified by RFI-IRFOS
SHA-256 (base APK)	`bf2618b5166bd58dbf3ffd263445adc266d542451296a191bf86112cc2f4dc80`

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: Exported push service without permission feeds microphone, log and lock commands on a child's device . . . 8

6.2 H1: Sound Around live microphone: bystander audio without notice, legal basis unresolved, audio path unconfirmed . . . 9

6.3 H2: Russian Trusted Root CA in the app-wide trust anchor, cleartext carve-out to a Russian carrier domain, Russian hosting named in the policy . . . 11

6.4 H3: Third-party code in the com.kids360 namespace provides app blocking and, in the audited build, the audio transport string set . . . 12

6.5 M1: Firebase API key, project and Realtime Database URL hardcoded in the distributed binary . . . 13

6.6 M2: Advertising-services permissions remain in the manifest, Crashlytics collection is not shown to wait for consent on a child's device . . . 14

6.7 M3: Accessibility service scope exceeds the stated screen time purpose . . . 15

6.8 O1: The monitored child cannot remove the app, and the company points to parental responsibility . . . 16

7 Impact Analysis 16

8 The Complete Chain 17

9 Data Protection: Article by Article 17

10 Consumer Protection & Platform Disclosures 18

11 Regulatory & Legal Landscape 18

12 Indicators of Compromise & Reproducible Evidence 19

13 Disclosure Timeline & Outcome 20

14 Operator Response of 16 November 2026 21

15 What Findmykids Got Right 22

16 Residual Risk & Recommendations 22

Executive Summary

Pingo is the child-side companion app of the Findmykids product family, installed on a device carried by a child or teenager at a parent's initiative. It is published by LETEM LTD in Nicosia, Cyprus, under the package org.findmykids.child and rated PEGI 3. The person whose microphone, location, call events and app usage the app governs is the child, who did not choose to install it and has no account. On 22 August 2026 RFI-IRFOS disclosed one Critical, three High and three Medium findings from a root level code analysis of version 2.11.96 under REF PINGO-2026-R1.

The Critical finding was an exported push service without a permission, which sat in front of the command that arms the child's microphone. Findmykids answered on 3 September 2026 that this is a security issue on its side and that it will close it. On 11 November 2026 it wrote a final response and stated that all measures are shipped in version 2.13.5. Google Play delivered version 2.13.6 to us, and our check of 14 November 2026 verified six items as closed: the push service and FirebaseMessagingService are not exported, the Russian Trusted Root CA is gone with no cleartext exception, no Selectel, selcdn, gdemoideti.ru or MegaFon reference remains, the AdMob key is gone, AppsFlyer is gone, and FCM auto-initialisation and Firebase Analytics collection are switched off.

Eight points were open after our verification. On 15 November 2026 we wrote again with the open points and repeated that the publication date stays 20 November 2026. On 16 November 2026 Findmykids answered each of the eight 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 the two advertising-services permissions (M2) are removed at manifest level and that Crashlytics collection starts only after consent, both in version 2.13.7 (build 2013070), 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 (M1) and the mapping file, described Kids360 as software deployed on its own servers in Hetzner (H3), named Falkenstein, Germany as the destination of the Sound Around stream, and holds to contractual necessity as the legal basis (H1). It also asked us to correct the record on the DPIA signatures. We did so on 17 November 2026. The point by point record is in the section on the operator response.

We reassessed two disclosed ratings downward after the verified fixes and the company's statements (H2, H3). The notice went to privacy@findmykids.org with support@findmykids.org, 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 2.11.96-google (versionCode 2011960): manifest, resources, network security configuration and the string pools of three classes*.dex files. The Google Play listing and the Findmykids Privacy Policy were read on 22 August 2026. Version 2.13.6 (build 2013060) was pulled from Google Play and compared by the same method for our message of 14 November 2026, which dates its text 11 November 2026. No account was created, no feature was exercised, no Findmykids 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 notice.

ID	Severity	Title
C1	CRITICAL	Exported push service without permission feeds microphone, log and lock commands on a child's device
H1	HIGH	Sound Around live microphone: bystander audio without notice, legal basis unresolved, audio path unconfirmed
H2	MEDIUM	Russian Trusted Root CA in the app-wide trust anchor, cleartext carve-out to a Russian carrier domain, Russian hosting named in the policy
H3	MEDIUM	Third-party code in the com.kids360 namespace provides app blocking and, in the audited build, the audio transport string set
M1	MEDIUM	Firebase API key, project and Realtime Database URL hardcoded in the distributed binary
M2	MEDIUM	Advertising-services permissions remain in the manifest, Crashlytics collection is not shown to wait for consent on a child's device
M3	MEDIUM	Accessibility service scope exceeds the stated screen time purpose
O1	INFO	The monitored child cannot remove the app, and the company points to parental responsibility

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	Fix verified in 2.13.6. Service not exported.
H1	HIGH	HIGH	Audio path: mapping file declined, functional description supplied, not verified. Legal basis, DPIA and region gate: operator declared closed, not verified.
H2	HIGH	MEDIUM	Root CA, Selectel, MegaFon, gdemoideti removed in 2.13.6. Resolved.
H3	HIGH	MEDIUM	Operator describes Kids360 as software on its own servers, not verified. Data categories stated.
M1	MEDIUM	MEDIUM	AdMob key removed. Firebase values remain. Operator declined restriction evidence, sent two Realtime Database screenshots.
M2	MEDIUM	MEDIUM	AppsFlyer removed. Removal of two permissions and Crashlytics consent stated for 2.13.7, not verified.
M3	MEDIUM	MEDIUM	Company position recorded. No change reported.
O1	Not in findings list	INFO	Both positions recorded. Not rated.

Subject & Operator Analysis

The Privacy Policy and the Play listing name LETEM LTD, Lakatameia, Nicosia 2324, Cyprus, as the operator of the Findmykids product family. 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. The parent-facing app org.findmykids.app is covered by a separate report, REF FINDMYKIDS-2026-R1.

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. Contact details of that authority are UNVERIFIED. RFI-IRFOS copies the Austrian DSB and the EDPS on the notice.

Findmykids stated that the code and the legacy signing certificates of the product were acquired from a Russian company and that Pingo uses the same codebase as Findmykids. The findings file records the product origin in Perm, Russia, with founders named in public sources.

Architecture & Data Flow

Pingo is a native Kotlin app with Jetpack Compose and Ktor networking and three dex files. It receives push commands through an app-authored Firebase listener and a PushHandlerInteractor that dispatches microphone, log retrieval, lock, allow-list, warning, SOS and COPPA state commands. The child-side components include a Device Admin lock, an Accessibility Service, a call screening service and the foreground microphone service for Sound Around. Location and activity recognition run in a dedicated geo process.

In the audited version 2.11.96 the audio transport strings sat in the com.kids360.websocket namespace. Findmykids states that Sound Around is based on its own technology and that Kids360 is not used for it. Findmykids also states that user data is processed on its own servers in Germany at Hetzner and that Kids360 may receive only anonymised statistical data. These are the company’s statements and they are not confirmed from the package.

The app models an explicit family structure with circles and roles. No NotificationListenerService was found. The relationship between parent and child is declared by design.

Engagement Summary

The notice REF PINGO-2026-R1 was sent on 22 August 2026 at 17:04 UTC to privacy@findmykids.org with support@findmykids.org, dsb@dsb.gv.at and edps@edps.europa.eu in copy. It listed six findings with exact classes, files and permissions and asked three questions.

Findmykids answered on 3 September 2026 through Egor Peresada, with colleagues in copy, in seven points, with fix dates before 10 November 2026 and a designated contact. A follow-up on 17 October 2026 referred to the 34 days remaining before publication. A final response of 11 November 2026 stated that all measures are implemented in version 2.13.5 (build 2013050). Our verification message of 14 November 2026 checked version 2.13.6 (build 2013060), which Google Play delivered, and lists six items closed and eight open points with a reply requested by 16 November 2026. The support desk answered that message with an automatic reply. Our message of 15 November 2026 repeated the eight open points and the publication date. The operator replied on 16 November 2026 in eight numbered points with four attachments.

Findings

C1: Exported push service without permission feeds microphone, log and lock commands on a child's device

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:P/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 5.8 (CVSS-B), disclosed as CRITICAL on 22 August 2026, acknowledged by Findmykids, fix verified in 2.13.6, rated CRITICAL by blast-radius escalation

In version 2.11.96 the manifest declares org.findmykids.pushes.google.FcmListenerService with exported true and no android:permission. It listens for com.google.firebase.MESSAGING_EVENT, the action that the SDK's own FirebaseMessagingService in the same manifest handles with exported false. Dex strings show the command family behind it: SoundChildPushHandler (microphone), LogSendPushHandler (remote log retrieval), LockedStatusPushHandler and WhitelistChildPushHandler (feature locking), WarningForceSendPushHandler, StopSosPushHandler and CoppaVerifiedPushHandler. Android places no restriction on which installed app may call an exported component without a permission. Whether the handlers check the origin of a delivered payload was not tested and a working forged command is not asserted. Findmykids answered on 3 September 2026: This is a security issue on our side, we will close it. Our check of 2.13.6 on 14 November 2026 confirmed that FcmListenerService is no longer exported and that FirebaseMessagingService is not exported either. The score reflects a local attacker app, an unverified handler check and one user step to install the attacker app. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.8 to CRITICAL because the component reaches a live microphone and remote lock commands on a minor's device, the operator itself calls it a security issue on its side, and exploitability stayed untested. The CVSS vector scores only the local exposure with an unverified handler check.

```
<service android:exported="true" android:name="org.findmykids.pushes.google.
    FcmListenerService">
    <intent-filter>
        <action android:name="com.google.firebase.MESSAGING_EVENT"/>
    </intent-filter>
</service>

<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>
```

```
registerLazyPushHandler:ChatsPushProcessor
registerLazyPushHandler:CoppaVerifiedPushHandler
registerLazyPushHandler:LockedStatusPushHandler:child
registerLazyPushHandler:LogSendPushHandler
registerLazyPushHandler:SoundChildPushHandler
registerLazyPushHandler:StopSosPushHandler
registerLazyPushHandler:WhitelistChildPushHandler
registerLazyPushHandler:WarningForceSendPushHandler:child
org.findmykids.app.domain.PushHandlerInteractor$processAntiRemovalIfNeeded$2
```

Impact: The service sat in front of the command that switches on a child's microphone. A parent expects that only the family account can do that. Until the update, the protection of the child's room depended on the app code behind an open door. Updated installs close that door.

Fix: Keep the service not exported, validate the origin of every delivered message, and state in writing which handler checks exist.

H1: Sound Around live microphone: bystander audio without notice, legal basis unresolved, audio path unconfirmed

---

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, Kids360 role denied by company, audio path pending, legal basis open, rated HIGH by blast-radius escalation

The child app runs ListeningService with foregroundServiceType microphone, started through SoundStarterActivity and reachable through SoundChildPushHandler. Version 2.11.96 carried audio over a JWT authenticated Ktor WebSocket client in the com.kids360.websocket namespace with a RoomConnection abstraction, which is a live relay. The Google Play listing describes the feature without a proximity qualifier. The Privacy Policy read on 22 August 2026 states that Sound Around works for 20 seconds when the parent is within 2 metres of the child's phone and that the company does not store sound around the device. The people recorded besides the child, siblings, classmates, teachers and other adults, receive no notice. Findmykids stated on 3 September and 11 November 2026 that Kids360 is not used for Sound Around, that the feature rests on its own technology, that no audio is recorded or stored, that a DPIA exists, that the legal basis is legitimate interest, that microphone sensitivity was reduced and that a pre-activation audible notification is a test in the United States and the United Kingdom. It also states that Sound Around is not available in Austria. Our check of 2.13.6 on 14 November 2026 could confirm ListeningService and SoundStarterActivity (package org.findmykids.soundaround) under plain names. The build is shrunk and renamed, so the audio path cannot be confirmed from the package until the R8 mapping file for build 2013060 is provided. The balancing test for non-user third parties is not part of the DPIA. The DPIA is version 1.0 dated 1 July 2023 and the file was created on 11 November 2026. Both signature lines (CTO, DPO) carry signature marks with no date beside them, and the signature annotations carry modification stamps of 11 November 2026. DPIA section 3.1 names Article 6(1)(b), while the message names legitimate interest. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the people recorded are children and bystanders who cannot consent, the feature is a live microphone on a minor's phone, and the app family is installed at large scale. The score is zero because the package shows no technical exposure of the audio to an attacker.

```
<activity android:name="org.findmykids.soundaround.childcore.starter.
    SoundStarterActivity" android:theme="@style/BlackWindow"/>
<service android:exported="false" android:foregroundServiceType="microphone" android:
    name="org.findmykids.soundaround.childcore.ListeningService"/>

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

```
com.kids360.websocket.api.JwtTokenPayload
com.kids360.websocket.api.JwtUserInfo
com.kids360.websocket.impl.DefaultSocketUrlProvider
com.kids360.websocket.impl.KtorRealtimeSocketClient
com.kids360.websocket.impl.KtorRealtimeSocketClient$RoomConnection
CHANNEL_SOUND_AROUND
CHANNEL_SOUND_AROUND_WITH_VOICE_UPDATED
org.findmykids.soundaround.child.stopByChild.ListeningStopFragment
org.findmykids.soundaround.child.stopByChild.why.ListeningStopWhyFragment
```

Privacy Policy as read on 22 August 2026 at findmykids.org/docs/privacy-policy/android/en, verbatim: The Company does not store sound around the device or audio data on any servers. Only the parent connected to the same child profile is allowed to access this information. Same policy: for 20 seconds (if You are within 2 meters of Your child's phone). Google Play listing, verbatim: Sound around - listen to what's going on around your child. This feature works only if the child tracker is installed and set up on their phone.

Impact: The feature turns a child's phone into a microphone for a parent. A sibling, a classmate or a teacher near that phone is recorded without being told. The child has a stop button, and the other people in the room have none.

Fix: Name one legal basis for the third-party audio, provide the balancing test, send the R8 mapping file for build 2013060, state the value and build of the microphone sensitivity reduction, publish the decision criteria and date for the pre-activation notification, and say where the region gate is enforced.

H2: Russian Trusted Root CA in the app-wide trust anchor, cleartext carve-out to a Russian carrier domain, Russian hosting 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 HIGH on 22 August 2026, reassessed after the explanation of 3 September and 11 November 2026, removal verified in 2.13.6

Version 2.11.96 trusted russian_trusted_root_ca in the base-config of the network security configuration for every TLS connection, permitted cleartext for megafon.gdemoideti.ru and held a Selectel CDN URL in the dex strings. The package visibility list names ru.gdemoideti.child and ru.gdemoideti.parent. The Privacy Policy read on 22 August 2026 named Selectel Ltd as a hosting provider and relied on standard contractual clauses. Findmykids explained on 3 September and 11 November 2026 that the code and legacy signing certificates were acquired from a Russian company, that the Root CA and the Selectel proxying path were meant to keep access for users in Russia, that the solution did not work and was removed, and that the data of Pingo users is processed in Germany at Hetzner. Our check of 2.13.6 on 14 November 2026 confirmed that the Root CA is gone (the configuration trusts system certificates and DST Root CA X3, with no cleartext exception) and that no reference to Selectel, selcdn, gdemoideti.ru or a MegaFon host remains in code or resources. The score covers the exposure that existed in 2.11.96 and is now removed.

```
<network-security-config>
    <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>
</network-security-config>
```

```
https://243408.selcdn.ru/userupload/todo-icons/todo_android_star.png
https://gdemoideti.onelink.me/BfYh/ulxbzdv1
```

Privacy Policy as read on 22 August 2026, verbatim: hosting services include Selectel Ltd, a company based in Russia. Transfers rely on standard contractual data protection clauses.

Impact: A child's app trusted a foreign state root certificate for all connections. A party able to present a certificate from that root on the network path could have read or altered traffic. The current version removes this possibility once installed.

Fix: Keep the configuration as in 2.13.6 and complete a Transfer Impact Assessment for any remaining non-EU recipient.

H3: Third-party code in the com.kids360 namespace provides app blocking and, in the audited build, the audio transport string set

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 HIGH on 22 August 2026, reassessed after the company statement of 3 September and 11 November 2026, data categories open

The manifest of 2.11.96 declares com.kids360.appBlocker services (GuardService, DeviceMonitorService, GuardActivity, PipGuardActivity, WakeUpDeviceMonitorReceiver). The package visibility list names app.kids360.parent and app.kids360.kid as external packages, and the public record lists the Kids360 consumer app under a different developer. Findmykids stated that Kids360 is used as an SDK that implements parental-control functionality inside the app, that Pingo receives and processes user data on its own servers, that Kids360 may receive only anonymised statistical data, that Kids360 is not used for Sound Around, and that Kids360 is now named in the Privacy Policy. Our check of 2.13.6 found the kids360.managed namespace still present. The data categories and fields that leave the device to Kids360 components, the method that makes them anonymous and whether any device, account or advertising ID belongs to them are open. Whether the relationship is a licence, a processor role or shared lineage was not determined from the package.

```
<service android:name="com.kids360.appBlocker.presentation.service.GuardService"/>
<service android:exported="false" android:name="com.kids360.appBlocker.presentation.
    service.DeviceMonitorService">
    <property android:name="android.app.PROPERTY_SPECIAL_USE_FGS_SUBTYPE" android:
    value="Our app uses foreground service to show a guard screens when kid plays or
    uses apps a lot of time..."/>
</service>
<activity android:name="com.kids360.appBlocker.presentation.activity.GuardActivity"
    .../>
<activity android:name="com.kids360.appBlocker.presentation.activity.PipGuardActivity"
     .../>
<receiver android:name="com.kids360.appBlocker.presentation.broadcastReceiver.
    WakeUpDeviceMonitorReceiver">
    <intent-filter><action android:name="android.intent.action.BOOT_COMPLETED"/></
    intent-filter>
</receiver>
```

Impact: A parent reading the notices could not learn that code from another company runs the blocking screens on the child’s phone. Whether that company receives any data from the child is the unanswered question.

Fix: List the data categories and fields shared with Kids360 components, state the anonymisation method and any identifiers involved, and name the role of Kids360 in the Article 30 record.

M1: Firebase API key, project and Realtime Database URL 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), open, restrictions not shown

res/values/strings.xml of 2.11.96 carries the values below. A Firebase key is not a secret by Google design, so the demonstrated exposure is availability through quota and billing exhaustion. Findmykids stated on 3 September and 11 November 2026 that the keys are restricted to the required APIs and to its authorised products by package name and signing certificate, that the Realtime Database is not used in Pingo and that the API was disabled in the Google Cloud Console. Our check of 2.13.6 found that the Firebase API key, the sender ID, the project and the Realtime Database URL remain in the build and that the AdMob application key is gone. The restriction and the disabled API cannot be seen from the package. Screenshots of the application and API restrictions, quota limits, App Check status and the Realtime Database API status were requested. No call was made against any project.

```
<string name="firebase_database_url">https://where-is-my-children.firebaseio.com</
    string>
<string name="gcm_defaultSenderId">339625562515</string>
<string name="google_api_key">AIzaSyDZp3fcu7xmJyoAHTFhQR5t47-W-4HNpOY</string>
<string name="google_app_id">1:339625562515:android:ad02d543179da7a5</string>
<string name="google_crash_reporting_api_key">AIzaSyDZp3fcu7xmJyoAHTFhQR5t47-W-4HNpOY
    </string>
<string name="project_id">where-is-my-children</string>
```

Impact: If the shared project were rate-limited, push messages and location features for families would be affected. The key stays in every installed copy until an update replaces it.

Fix: Show the key restrictions and App Check status, confirm deny-by-default rules or a disabled Realtime Database, and remove values the app no longer uses.

M2: Advertising-services permissions remain in the manifest, Crashlytics collection is not shown to wait for consent on a child's device

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, AppsFlyer removed in 2.13.6, permissions and Crashlytics open

Version 2.11.96 declared ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID and the Play install referrer binding, an AppsFlyer OneLink domain and Google Mobile Ads consent string plumbing (IABTCF_CmpSdkID, IABTCF_TCString, IABTCF_gdprApplies, IABTCF_PurposeConsents, dma_consent_state). The Google Play permission justification lists four reasons and mentions no advertising or attribution processing. Findmykids stated on 3 September 2026 that AppsFlyer should not be in Pingo and on 11 November 2026 that AppsFlyer and the advertising-services permission were removed. Our check of 2.13.6 confirmed that AppsFlyer is gone and that FCM auto-initialisation and Firebase Analytics collection are off in the manifest. The manifest of 2.13.6 still declares ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION, so the statement that the permission was removed does not match the build. The Crashlytics components are registered and the manifest holds no firebase_crashlytics_collection_enabled entry. Firebase documents that Crashlytics collects crash reports for all users by default. Whether collection is active before consent on a child's device and on which legal basis is open. This is a transparency finding with no technical vector.

```
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_ATTRIBUTION"/>
<uses-permission android:name="android.permission.ACCESS_ADSERVICES_AD_ID"/>
<uses-permission android:name="com.google.android.finsky.permission.
    BIND_GET_INSTALL_REFERRER_SERVICE"/>

https://gdemoideti.onelink.me/BfYh/ulxbzdv1
IABTCF_CmpSdkID, IABTCF_TCString, IABTCF_gdprApplies, IABTCF_PurposeConsents
ALTER TABLE apps ADD COLUMN dma_consent_state INTEGER;
```

Impact: An advertising identifier permission on a child's phone suggests that a child can be recognised across apps. No ad display was found, and the permission is unexplained for the family that installs the app.

Fix: Remove the two advertising-services permissions or name the component that needs them, and gate Crashlytics on a recorded consent event on the child's device.

M3: Accessibility service scope exceeds the stated screen time purpose

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, company position recorded, open

The manifest declares org.findmykids.appBlock.AppAccessibilityService with BIND_ACCESSIBILITY_SERVICE, together with PACKAGE_USAGE_STATS and QUERY_ALL_PACKAGES. The stated purpose on Google Play is Screen time manager. The Accessibility API can in principle read on-screen text and interface content across foreground apps. Findmykids stated on 3 September and 11 November 2026 that screen content, down to text on the screen, is needed for parental control, that it is not continuously collected or stored and that it is read where a restriction must be applied, for example in device settings or a browser. The capability is shown by the package. Whether the implementation reads content beyond that purpose was not tested and is not asserted. The item was not part of the open points of 14 November 2026.

```
<service android:exported="false" android:name="org.findmykids.appBlock.
    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>

android.permission.PACKAGE_USAGE_STATS
android.permission.QUERY_ALL_PACKAGES
```

Impact: The same access that allows blocking on a child’s phone can in principle read the text of private conversations. The child carries that on a personal device.

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

O1: The monitored child cannot remove the app, and the company points to parental responsibility

INFO, no CVSS v4.0 score assigned, observation from the notice of 22 August 2026, not rated

The manifest and the device admin description text state that the app protects itself from being uninstalled and allows enforcing device lock. The notice of 22 August 2026 described the child as someone who did not choose to install the app and is technically resisted from removing it. Findmykids answered on 3 September and 11 November 2026 that parental control and restrictions on deleting the application follow from the parents' responsibility, that intra-family disagreements are for parents and children to resolve, and that the child can stop an active Sound Around session and can disable the application's microphone access in device settings. The report records both positions and does not rate the design choice. The child facing ListeningStopFragment and ListeningStopWhyFragment give the child a visible stop control for Sound Around.

```
Protects the app from being uninstalled and allows enforcing device lock
```

Impact: A child who disagrees with a restriction cannot lift it alone. The company treats that as a family matter, and the other side of the question is the child's voice in a product that watches them.

Fix: Document how the child can see which restrictions and which monitoring functions are active.

Impact Analysis

The people affected are children and teenagers who carry the app, parents who rely on it, and anyone within earshot of the child's phone when Sound Around runs. The child is not the account holder and cannot consent. The feature set is broad: location, activity and sleep signals, an anti-removal Device Admin, an accessibility service and a live microphone.

In version 2.11.96 the largest structural exposures were the exported push service in front of the microphone command (C1) and the Russian root certificate in the app-wide trust anchor (H2). Both are closed in 2.13.6. The remaining weight sits on Sound Around (H1), because it records people who have no relationship with the operator, and on the transparency of the advertising permissions, Crashlytics and Kids360 (M2, H3).

The demonstrated harm is a harm of configuration and transparency. No forged command was sent, no audio was captured and no access to any account was tried.

The Complete Chain

Step 1, install: a parent links the child app to the family account through a pairing flow with a COPPA verified parental consent state.

Step 2, standing state: Firebase components and Crashlytics are registered. In 2.13.6 FCM auto-initialisation and Firebase Analytics collection are off, and Crashlytics is not shown to be gated in the version we checked (M2). The operator states that version 2.13.7 gates it on consent.

Step 3, commands: in 2.11.96 the push listener was exported without a permission and dispatched the command family (C1). In 2.13.6 it is not exported.

Step 4, Sound Around: the parent triggers a live microphone session. The child can stop it and sees why. Bystanders get no notice (H1). The legal basis is stated two ways.

Step 5, blocking: the accessibility service and the Kids360 code run the guard screens on the child's device (M3, H3).

Step 6, the child tries to remove the app: the Device Admin resists removal, which the company treats as parental responsibility (O1).

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by H1 and M2.

Article 5(1)(c), data minimisation: engaged by H1 and M3.

Article 5(1)(f), integrity and confidentiality: engaged by C1.

Article 5(2), accountability: engaged by H3.

Article 6(1), lawful basis: engaged by H1 and M2. Article 6(1)(b) in DPIA section 3.1 against legitimate interest under Article 6(1)(f) in the company's message is the open question. The operator stated on 16 November 2026 that contractual necessity is the only legal basis and attached an internal legitimate interest assessment that states it does not change that reliance.

Article 7(1), conditions for consent: engaged by M2.

Article 9: engaged by H1 as a question for voice data of bystanders. No special category processing is asserted.

Articles 13 and 14: engaged by H1, H3 and M2.

Article 25: engaged by C1, M1 and M3.

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

Article 28: engaged by H3, where the role of Kids360 is the open question. The operator states that LETEM LTD operates the Kids360 server components itself and that Kids360 developers receive only aggregated statistics.

Article 32(1)(a) and (b): engaged by C1, H2 and M1.

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 later size-optimisation step for a transmission copy and not the approval date. The balancing test for non-user third parties is not in it. The operator listed the DPIA sections that deal with bystanders.

Articles 44 and 46: engaged by H2. The company states that data stays in Germany and the Russian components are removed.

ePrivacy Directive Article 5(3): engaged by M2.

Consumer Protection & Platform Disclosures

The Google Play permission justification lists four reasons for the permissions and mentions no advertising or attribution processing, while the manifest declared advertising-services permissions (M2). The permissions remain in 2.13.6. The operator states that 2.13.7 removes them.

The Play listing describes Sound Around without a proximity qualifier, and the Privacy Policy describes it as working for 20 seconds within 2 metres of the child's phone (H1). The two public descriptions of the same feature differ. The current Data Safety section of the listing was not re-read for this report.

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, 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.child
Version audited    2.11.96-google (versionCode 2011960), analysed 2026-08-22
base APK SHA-256   bf2618b5166bd58dbf3ffd263445adc266d542451296a191bf86112cc2f4dc80
XAPK SHA-256       26f9c44fc4b546a880a87b1150eb4fa30df05866105cc66d182e4743405858ff
minSdk / targetSdk 29 / 36

Version checked    2.13.6 (build 2013060), pulled from Google Play for the message of
    2026-11-14
base.apk SHA-256   6c28b3760a6863dab86846d34680bb07f158aeb75e5faec21973b2df27be7770
split_config.arm64_v8a.apk SHA-256  9966
    ec95e9fc44af47f4c8b53f262cfa51a35a01f66f486df8df553a9bf1b000
split_config.xxhdpi.apk SHA-256     970
    b58ee4645ffe03b63cb097872aa36452f6734c3b8e35d7473b8cd42bfa8f0

Firebase project   where-is-my-children
google_api_key     AIzaSyDZp3fcu7xmJyoAHTFhQR5t47-W-4HNpOY
google_app_id      1:339625562515:android:ad02d543179da7a5
gcm_defaultSenderId 339625562515
Database URL       https://where-is-my-children.firebaseio.com
Selectel URL       https://243408.selcdn.ru/userupload/todo-icons/todo_android_star.
    png
Offer link         https://gdemoideti.onelink.me/BfYh/ulxbzdv1
```

```
C1  AndroidManifest.xml (FcmListenerService, FirebaseMessagingService), dex strings (
    PushHandler family)
H1  AndroidManifest.xml (ListeningService, SoundStarterActivity), dex strings (kids360
    .websocket, ListeningStopFragment), Privacy Policy, Google Play listing
H2  res/xml/network_security_config.xml, dex strings (selcdn URL), Privacy Policy
    hosting section
H3  AndroidManifest.xml (com.kids360.appBlocker), package visibility list
M1  res/values/strings.xml
M2  AndroidManifest.xml (ACCESS_ADSERVICES permissions), dex strings (OneLink, IABTCF)
    , Google Play permission justification
M3  AndroidManifest.xml (AppAccessibilityService)
O1  Device admin description text, ListeningStopFragment
```

Reproduction: obtain org.findmykids.child 2.11.96-google, check the SHA-256 above, decode the manifest and resources with apktool and read the named files. The same steps with 2.13.6 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 PINGO-2026-R1 at 17:04 UTC to privacy@findmykids.org, CC support@findmykids.org, DSB and EDPS. Six findings, three questions, written response requested within 30 days.

2026-09-03 Substantive reply from Egor Peresada in seven points. The exported service is called a security issue on the company's side that will be closed. Fix dates before 10 November 2026 and a designated contact.

2026-10-17 Follow-up from security@rfi-irfos.com, 34 days before the embargo date and 56 days after the notice.

2026-11-11 Final response of Findmykids: all measures in version 2.13.5 (build 2013050).

2026-11-14 Our verification message on version 2.13.6 (build 2013060): six items closed, eight points open, reply requested by 16 November 2026. An automatic reply from the support desk followed within a minute and gave no reply on the findings.

2026-11-15 Message from security@rfi-irfos.com at 14:08 UTC, five days before the embargo date, repeating the eight open points and stating that the publication date remains 20 November 2026.

2026-11-16 Reply from Egor Peresada at 16:24 UTC in eight numbered points, each declared closed by the operator. Version 2.13.7 (build 2013070) 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 16:24 UTC. The thread holds eight messages: four from RFI-IRFOS, three human replies and one automatic reply from the operator.

Operator Response of 16 November 2026

Statements of the operator, reply of 16 November 2026 (Egor Peresada, 16:24 UTC, REF PINGO-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. Advertising permissions. The two permissions come in through transitive dependencies and are not used. ”We have removed these permissions at manifest level using tools:node= ”remove”.” The change is in version 2.13.7 (build 2013070), submitted on 16 November 2026. We did not pull it. Status for RFI-IRFOS: open until the build is checked.

2. Crashlytics and consent. ”Crashlytics is handled in the same way as Firebase Analytics.” The change is part of 2.13.7. Status: open until the build is checked.

3. 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.

4. Kids360. The SDK is integrated and the server software runs in LETEM LTD infrastructure in Hetzner data centres. ”Personal data of Pingo users are not transferred to the Kids360 developers.” The components process the installed applications and the application use on the child device, and the developers receive aggregated, anonymised statistics. The operator states that Kids360 is now in the Pingo Privacy Policy. Status: statement recorded, not verified.

5. 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 the operator states that a JWT identifies the user inside the TLS connection and 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.

6. Legal basis, balancing test, DPIA. The operator relies on Article 6(1)(b) only and states that the DPIA was approved on 1 July 2023 and signed. It states that the PDF timestamp reflects a size-optimisation step. 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.

7. Microphone sensitivity. ”The sensitivity level was reduced from 5.5 to 1.75”, stated as present in 2.13.6. The audible pre-activation notification ”remains under evaluation” with no fixed decision date. Status: value not verified at the build.

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

What Findmykids Got Right

Findmykids called the exported service a security issue on its side within two weeks and shipped the fix. The Root CA, the Selectel path, the MegaFon and gdemoideti references, the AdMob key and AppsFlyer are removed in 2.13.6, and FCM auto-initialisation and Firebase Analytics collection are off. The child receives a visible stop control for Sound Around with an explanation of why it was triggered. A COPPA verified parental consent architecture exists, with a date of birth, a required state and a blocked screen. Backup is excluded for all data domains in cloud backup and device transfer, and allowBackup is false. A real Article 27 representative is named in Bremen. The company named a designated technical contact, gave class by class answers for the audio path of the parent app and told us the build number. On 16 November 2026 it answered all eight 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 14 November 2026 and the findings above: the advertising-services permissions (M2), Crashlytics collection control (M2), the key restrictions with App Check and the Realtime Database API status (M1), the data categories shared with Kids360 (H3), the R8 mapping file and transport destination for Sound Around (H1), the single legal basis, the balancing test and the DPIA approval (H1), the build and value of the microphone sensitivity reduction and the criteria and date for the pre-activation notification (H1), and the location of the region gate (H1).

Recommendations: remove the two advertising-services permissions or name the component that needs them, gate Crashlytics on the consent event, show restriction and App Check evidence for the Firebase key, list the Kids360 data categories and the anonymisation method, send the mapping file, name one legal basis for Sound Around and provide the balancing test, approve and sign the DPIA, and publish the decision criteria for the pre-activation notification.

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 servers, devices or accounts were probed. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. REF PINGO-2026-R1.