Security & Privacy Disclosure, Final Report

CuboAi Smart Baby Monitor for Android (com.getcubo.app)

A baby monitor that keeps raw video on the camera for 18 hours, with analytics that start before any consent and an EU contact in London.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO DATE 20 NOVEMBER 2026 REACHED. ONLY AN AUTOMATED SUPPORT TICKET REPLY, NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.

Target	Yun Yun AI Baby Camera Co., Ltd. (CuboAi), Taipei, Taiwan
Version Audited	2.27.0 / 2492 (2026-08-22)
EU Representative	Named as VeraSafe United Kingdom Ltd., London (not in the EU)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days)
Findings	6: 1 Critical, 2 High, 2 Medium, 1 observation
Status	No substantive reply as of 21 November 2026. The only inbound message is an automated support ticket reply of 18 October 2026.
SHA-256 (base APK)	`302ac3487a7ab15b0930ecba5ad81826a8dfe422fedc406e465a6d93fb45a085`

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

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 5

5 Engagement Summary 6

6 Findings 7

6.1 C1: Firebase and Google Measurement start with the app process, before any consent screen, with no consent platform in the binary, on a paid product . . . 7

6.2 H1: Article 27 representative named in the privacy policy is established in London, outside the European Union . . . 8

6.3 H2: Hardcoded Firebase API key, live Realtime Database URL and Cloud Storage bucket for the project that holds infant thumbnails . . . 9

6.4 H3: Health-adjacent monitoring of a child: specific Article 9(2)(a) consent exists, impact assessment and processing location are open questions . . . 10

6.5 M1: Live camera transport runs on ThroughTek IOTC P2P, a product class with a documented vulnerability history, SDK version not shown . . . 11

6.6 M2: No certificate pinning for any backend channel, network security configuration otherwise clean . . . 12

7 Impact Analysis 12

8 The Complete Chain 13

9 Data Protection: Article by Article 13

10 Consumer Protection & Platform Disclosures 14

11 Regulatory & Legal Landscape 14

12 Indicators of Compromise & Reproducible Evidence 15

13 Disclosure Timeline & Outcome 16

14 What CuboAi Got Right 16

15 Residual Risk & Recommendations 16

Executive Summary

CuboAi Smart Baby Monitor is the companion app for a camera and a sleep sensor pad that watch over infants. It is published on Google Play by Yun Yun AI Baby Camera Co., Ltd. of Taipei under the package com.getcubo.app, rated PEGI 3 with in-app purchases. On 22 August 2026 RFI-IRFOS disclosed six findings from a root level code analysis of version 2.27.0 under REF CUBOAI-2026-R1.

The architecture is better than most of its class. Raw video stays on the camera for 18 hours and is then deleted, only safety event thumbnails go to Google Cloud for 7 days, a specific Article 9(2)(a) consent step guards breathing and sleep analysis, cleartext traffic is denied everywhere, and the privacy policy names its processors including ThroughTek. The findings sit beside that design and not against it.

Three findings are open and carry the weight. Firebase analytics and crash reporting start with the process, before any consent screen, and the binary holds no consent platform (C1). The privacy policy names a representative in London as the EU contact, which Article 27(1) does not allow (H1). A hardcoded Firebase key belongs to a project whose storage holds thumbnails that may show babies' faces (H2). The people behind these findings are parents who pay for the service and infants who cannot consent.

The notice of 22 August 2026 went to three CuboAi addresses with the Austrian DSB and the EDPS in copy. Follow-ups on 17 October 2026 and 15 November 2026 repeated the three questions and named the embargo date. The only message received is a support ticket reply of 18 October 2026 that routes the sender to collaboration and press addresses. No finding and no question has been answered. This report is published after the embargo date of 20 November 2026 was reached.

Scope: Root level code analysis of the Google Play release 2.27.0 (versionCode 2492): manifest, resources, dex string pool. The privacy policy at us.getcubo.com/pages/privacy-policy and the assetlinks.json on app.getcubo.com were read from the public sites on 22 August 2026. No CuboAi server, database or bucket was called, no account was created, no traffic was intercepted and no runtime instrumentation was used. Items the package cannot show are marked UNVERIFIED.

ID	Severity	Title
C1	CRITICAL	Firebase and Google Measurement start with the app process, before any consent screen, with no consent platform in the binary, on a paid product
H1	HIGH	Article 27 representative named in the privacy policy is established in London, outside the European Union
H2	HIGH	Hardcoded Firebase API key, live Realtime Database URL and Cloud Storage bucket for the project that holds infant thumbnails
H3	INFO	Health-adjacent monitoring of a child: specific Article 9(2)(a) consent exists, impact assessment and processing location are open questions
M1	MEDIUM	Live camera transport runs on ThroughTek IOTC P2P, a product class with a documented vulnerability history, SDK version not shown
M2	MEDIUM	No certificate pinning for any backend channel, network security configuration otherwise clean

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	CRITICAL	Open. No answer received. Version 2.27.0 analysed on 22 August 2026.
H1	HIGH	HIGH	Open. No answer received.
H2	HIGH	HIGH	Open. No answer received.
H3	HIGH (noted)	INFO	Observation. Two questions unanswered.
M1	MEDIUM	MEDIUM	Open as a question to the operator.
M2	MEDIUM	MEDIUM	Open. No answer received.

Subject & Operator Analysis

The privacy policy names Yun Yun AI Baby Camera Co., Ltd. as controller, registered at Rm. 4, 19F., No. 2, Ln. 150, Sec. 5, Xinyi Rd., Xinyi Dist., Taipei City 110014, Taiwan (R.O.C.). The policy lists business@cuboai.com, support@cuboai.com and support@getcubo.com as contacts. A separate contact for regulatory matters and a data protection officer are not named beyond the representative channel. The package namespace cloud.yunyun is the controller's own name and not a third-party vendor.

No EU establishment appears on the public record, so no lead supervisory authority under the one-stop-shop applies. For an Austrian initiated matter the competent authority is the Österreichische Datenschutzbehörde. The policy names VeraSafe United Kingdom Ltd., 37 Albert Embankment, London SE1 7TL, as representative in the European Union, reachable through a web form (H1).

The app is signed with the Google Play App Signing certificate 59:AB:B9:4E:E4:72:28:09:5E:ED:A3:B7:EC:08:BA:65:09:D8:94:ED:4B:BB:27:D2:22:FA:99:29:4A:5A:71:C3, which matches the assetlinks.json served from app.getcubo.com. The deep-link ownership chain is clean.

Architecture & Data Flow

CuboAi Smart Baby Monitor is a native Kotlin and Java app with nine dex files and no bundled machine learning models. Live video, audio and camera control run over the ThroughTek IOTC peer to peer protocol through the controller's own TutkEndpoint wrapper. Cry, face cover and rollover detection are requested through IOTC messages, and a DNN confidence level is exposed as a user setting. This points to inference on the camera and on the sleep sensor pad, which the package cannot prove because the firmware is outside the analysis.

Per the privacy policy, raw video stays on the camera for 18 hours and is then deleted. Safety event thumbnails, which may include partial face images, are stored on Google Cloud Platform for 7 days so that users can review events. Face data is processed on the operator's servers and is not shared with third parties.

The app also integrates Firebase (project cubo-smart-baby-camera) with ten registered subsystems, AWS Cognito, Google Play Billing 7.0.0 for subscription plans, and api.getcubo.com. Firebase starts from a ContentProvider before any Activity (C1). Network traffic is HTTPS only by configuration, without pinning (M2).

Engagement Summary

The notice REF CUBOAI-2026-R1 was sent on 22 August 2026 at 12:53 UTC to business@cuboai.com, support@cuboai.com and support@getcubo.com, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It listed C1, H1, H2 and H3 with verbatim evidence, summarised two medium findings, credited the video retention design, and asked three questions.

A follow-up with the same three questions went to the same addresses on 17 October 2026, 34 days before the embargo date, and a final notice of the embargo date followed on 15 November 2026 (12:58 UTC) from s.kepp@rfi-irfos.com. On 18 October 2026 at 20:38 UTC the support desk answered through its ticket system under the subject Collaboration. That message thanks the sender for interest in working together and names KOL and press addresses for collaboration requests. It does not mention any finding or question.

No other message from CuboAi or from a representative is on record. All three questions remain open.

Findings

C1: Firebase and Google Measurement start with the app process, before any consent screen, with no consent platform in the binary, on a paid product

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, rated CRITICAL by blast-radius escalation

FirebaseInitProvider is declared directBootAware with initOrder 100, so Firebase registers before any Activity can draw a consent screen. Ten Firebase subsystems register through ComponentDiscoveryService, among them Analytics, Crashlytics, Messaging, Remote Config, Storage and App Check. A search of the resource strings and all nine classes*.dex files for OneTrust, Didomi, Usercentrics, consentmanager and IAB TCF returned zero hits. Scope: this finding covers general app telemetry. It does not cover the video and audio stream and it does not cover the separate Article 9(2)(a) consent step for breathing and sleep monitoring, which exists and is credited below. The content of the telemetry was not measured, no traffic was captured. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the monitored person is an infant who cannot consent, the household pays for the product, initialisation can occur before the device is unlocked, and no consent mechanism of any kind exists in the binary. The CVSS vector scores only the technical exposure of low-sensitivity telemetry.

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

<receiver android:name="com.google.android.gms.measurement.AppMeasurementReceiver"
    android:enabled="true" android:exported="false"/>
<service android:name="com.google.android.gms.measurement.AppMeasurementService"
    android:enabled="true" android:exported="false"/>
<service android:name="com.google.android.gms.measurement.AppMeasurementJobService"
    android:enabled="true" android:exported="false"
         android:permission="android.permission.BIND_JOB_SERVICE"/>

com.google.android.gms.permission.AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_AD_ID

grep -i "onetrust|didomi|usercentrics|consentmanager|iabtcf"  (resources + 9 dex files
    )  ->  0 hits
```

The app sells paid subscription plans through Google Play Billing 7.0.0 (CuboAi Plus, CuboAi Ultimate and Care). The common argument that tracking pays for a free app does not apply. Initialisation is identical for a paying household and for one that never pays.

Impact: A household that pays to watch over an infant has no choice to make about telemetry, because the telemetry starts when the app process starts. The app is used in a nursery, and install and usage signals from that device go to Google services before anyone has been asked.

Fix: Disable automatic collection in the manifest, initialise Firebase Analytics and Crashlytics only after a recorded consent decision, and apply the same gate to paying and non-paying households. The advertising identifier permissions need a stated purpose or removal.

H1: Article 27 representative named in the privacy policy is established in London, outside the European Union

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), open, rated HIGH by blast-radius escalation

The privacy policy at us.getcubo.com/pages/privacy-policy, read on 22 August 2026, states: Our representative in the European Union is VeraSafe United Kingdom Ltd., address at 37 Albert Embankment, London SE1 7TL, United Kingdom. The United Kingdom has not been an EU Member State since 31 January 2020. Article 27(1) requires the representative to be established in one of the Member States where the data subjects are. The controller is Yun Yun AI Baby Camera Co., Ltd. in Taipei, which has no EU establishment on the public record. This is a legal and transparency finding with no technical attack path, so the CVSS vector carries no impact. RFI-IRFOS blast-radius escalation: raised from none to HIGH because the data concerns infants, the rights holders are their parents, and the named role cannot be exercised from the stated address under Article 27(1). The score is zero because no technical vector exists.

```
The privacy policy applies to the processing of personal data by Yun Yun AI Baby
    camera Co., Ltd.
with registered offices at Rm. 4, 19F., No. 2, Ln. 150, Sec. 5, Xinyi Rd., Xinyi Dist
    ., Taipei City
110014, Taiwan (R.O.C.) ("we", "Yun Yun"). Yun Yun is a controller in the meaning of
    the GDPR.
Our representative in the European Union is VeraSafe United Kingdom Ltd., address at
    37 Albert
Embankment, London SE1 7TL, United Kingdom.
```

Impact: A parent in the EU who wants access to, or erasure of, images and sleep data about their baby is given a London address as the EU contact. Supervisory authorities have no Member State address to write to. The people who need the representative most are the ones who hold data about a child.

Fix: Designate a representative established in a Member State where monitored households live and publish it in the policy the app links to. Publish the name of a data protection contact.

H2: Hardcoded Firebase API key, live Realtime Database URL and Cloud Storage bucket for the project that holds infant thumbnails

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, rated HIGH by blast-radius escalation

res/values/strings.xml of version 2.27.0 carries the Firebase API key, the project ID, the app ID, the sender ID, the Realtime Database URL and the Cloud Storage bucket in plain text. A Firebase key is not a secret by Google design, so the demonstrated exposure is availability: quota and billing exhaustion against the project. The privacy policy states that safety event thumbnails are stored on Google Cloud Platform for 7 days and may include partial face images. Whether the Security Rules for the Realtime Database and the bucket restrict read and write access is not shown by the package, and no call was made against the project. App Check is compiled in, whether it is enforced server-side is a question for the controller. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the project is documented by the operator as storing facial thumbnails of infants and the key cannot be rotated for installed copies. The CVSS vector scores only the demonstrated availability exposure.

```
<string name="google_api_key">AIzaSyARGu__5GvluNV0zCkNHdqQhgMw7O58YiM</string>
<string name="google_crash_reporting_api_key">AIzaSyARGu__5GvluNV0zCkNHdqQhgMw7O58YiM
    </string>
<string name="google_app_id">1:1024118653750:android:f82ad8e3e67f1ad5</string>
<string name="project_id">cubo-smart-baby-camera</string>
<string name="google_storage_bucket">cubo-smart-baby-camera.appspot.com</string>
<string name="firebase_database_url">https://cubo-smart-baby-camera.firebaseio.com</
    string>
<string name="gcm_defaultSenderId">1024118653750</string>
<string name="default_web_client_id">1024118653750-n1qo0hi2800ah6cmvod2ui6uhkr954i9.
    apps.googleusercontent.com</string>
```

Impact: The key is in every installed copy and cannot be rotated without an app update. If the project is rate-limited or billed out, the safety event notifications that parents rely on stop. The bucket the key belongs to holds thumbnails of babies, which makes correct storage rules a matter for the controller to demonstrate.

Fix: Restrict the key by package name, signing certificate and API scope, enforce App Check for Realtime Database and Storage, and send the Security Rules and quota settings as evidence.

H3: Health-adjacent monitoring of a child: specific Article 9(2)(a) consent exists, impact assessment and processing location are open questions

INFO, no CVSS v4.0 score assigned, noted rather than penalized in the notice of 22 August 2026

The app presents a specific consent string for tracking and analysing a child's breathing motion and sleeping patterns. The privacy policy names Article 9(2)(a) as the legal basis. The camera reports cry, cover and rollover detection through ThroughTek IOTC messages, and a Sleep Sensor Pad reports through its own message set. The package does not show where classification runs, because that logic sits in camera and pad firmware. The notice asked two questions: whether an Article 35 impact assessment exists, and whether classification runs only on the hardware. No answer has been received. This item is recorded as an observation and carries no severity score, because a missing document is not shown by the binary.

```
<string name="gdpr_sa_agreement_term_android">I consent to CuboAi tracking and
    analyzing my
child's breathing motion and sleeping patterns. I am the child's legal representative
    or have
been authorized by the legal representative of the child to consent to this. For more
information, I refer to the <TAG>Terms of Service</TAG> and
<TAG>Privacy Policy</TAG>.</string>

com/getcubo/app/v2/features/breathing/PadViewModel$pairMat
com/getcubo/app/v2/features/breathing/PadViewModel$setAiMode
Lcom/tutk/IOTC/messages/SMsgAVIoctrlGetSleepSafetyStatusReq;
Lcom/tutk/IOTC/messages/SMsgAVIoctrlGetMatInfoReq;
Lcom/tutk/IOTC/messages/SMsgAVIoctrlGetCryDetectReq;
setting_cry_detection_dnn_confidence_level_title_tv
```

Impact: Breathing and sleep signals of a baby are about as close to health data as a home camera gets. The parent is asked for specific consent, which is the right design. What the parent cannot see is whether a documented impact assessment stands behind it.

Fix: Answer the two questions in writing, and publish the Article 35 outcome or a summary of it.

M1: Live camera transport runs on ThroughTek IOTC P2P, a product class with a documented vulnerability history, SDK version not shown

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as MEDIUM, open, held as a question to the operator

Live video and audio use the ThroughTek IOTC SDK (package com.tutk.IOTC, wrapper cloud.yunyun.cubo.camera.endpoint.TutkEndpoint). The product class was affected by CVE-2021-32934 (CISA advisory ICSA-21-292-01), which allowed remote access to live streams through device UID enumeration before AuthKey authentication was introduced. The binary contains AuthKey error codes, which is consistent with a build that uses the newer authentication. The exact SDK version and whether AuthKey is mandatory for every camera are not shown by the package. UNVERIFIED, no dynamic test was made. The yunyun namespace is the operator's own name and not a third party.

```
Lcloud/yunyun/cubo/camera/endpoint/TutkEndpoint;
Lcom/tutk/IOTC/AVAPIs$avTokenAuthFn;
Lcom/tutk/IOTC/AVAPIs$avChangePasswordRequestFn;
Lcom/tutk/IOTC/AVAPIs$avEnableVSaaS
IOTC_ER_DID_NOT_LOGIN_WITH_AUTHKEY
IOTC_ER_DEVICE_REJECT_BY_WRONG_AUTH_KEY
IOTC_ER_DEVICE_NOT_USE_KEY_AUTHENTICATION
```

Impact: The stream carries live images and sound from a nursery. If an old SDK generation were present on a camera, the room could be watched by someone other than the parents. The binary points to the newer generation, so this is a question to the operator and not an assertion.

Fix: State the SDK version and confirm AuthKey enforcement for every camera model in the product line.

M2: No certificate pinning for any backend channel, network security configuration otherwise clean

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, open, rated MEDIUM by blast-radius escalation

The network security configuration denies cleartext traffic globally with no domain exception, which is correct and credited below. It declares system trust anchors only and no pin-set. The app talks to Firebase, AWS Cognito, ThroughTek services and api.getcubo.com. Without pinning, an attacker who controls a trust anchor on the device, or a network position combined with a mis-issued certificate, can interpose on those connections. RFI-IRFOS blast-radius escalation: raised from LOW/2.3 to MEDIUM because the credentials and pairing state protected by these channels give access to a camera in a child's room. The vector scores the attacker position that is required.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="false">
        <trust-anchors>
            <certificates src="system" />
        </trust-anchors>
    </base-config>
</network-security-config>
```

Impact: The credentials and pairing state of a baby monitor are the keys to a camera in a child's room. Pinning would narrow the places where those can be intercepted. The gap is real and the attacker needs a strong position.

Fix: Add a pin-set for api.getcubo.com and for the backends the operator controls.

Impact Analysis

The people affected are parents who bought a camera for a nursery and the infants they watch. The product is paid, so the people who bear the cost of weak consent handling are also customers. Infants are never a party to any consent. The app carries no ad mediation stack, so the telemetry of C1 serves measurement and not advertising display.

C1 affects every user of the app on every launch. H1 affects every parent who tries to exercise a right against the controller, and the supervisory authority that tries to reach the representative. H2 affects the availability of the service for all users and sits next to a store of infant thumbnails whose access rules the package does not show. M1 and M2 concern the paths through which live images and credentials travel.

The demonstrated harm is a harm of design and transparency. No access to footage, thumbnails or accounts was shown, and none was tried.

The Complete Chain

Step 1, purchase and install: a household buys a CuboAi camera, installs the app from Google Play, and may buy a subscription plan through Play Billing (C1).

Step 2, first launch: FirebaseInitProvider starts with the process, before any screen, and can start before the device is unlocked. Analytics, Crashlytics and Measurement register with the app. No consent step precedes them (C1).

Step 3, pairing and consent: the app asks the parent for a specific consent to the analysis of the child's breathing and sleep. This step is well formed and is separate from step 2.

Step 4, operation: live video and audio travel over ThroughTek IOTC. Safety event thumbnails go to Google Cloud Platform for 7 days. The app reaches api.getcubo.com, AWS Cognito and Firebase without pinning (M1, M2, H2).

Step 5, the parent tries to act: the policy gives a London address as EU representative (H1). Whether an impact assessment exists for the sleep analysis is not stated anywhere the parent can read (H3).

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1 and H1.

Article 5(2), accountability: engaged by C1, H1 and H2. The controller carries the burden of showing consent gating, a valid representative and correct storage rules.

Article 6(1) and Article 7(1), lawful basis and conditions for consent: engaged by C1. Telemetry that starts before a consent decision has no consent to rest on. The notice asked for the technical measure.

Article 8, child's consent: touched by H3. The account holder gives consent as legal representative, which the consent string states.

Article 9(2)(a), explicit consent for special categories: met in form for breathing and sleep analysis, by the in-app consent string and the privacy policy.

Article 25, data protection by design and by default: engaged by C1 and H2.

Article 27(1) and (3), representative: engaged by H1. A representative established in London does not meet the requirement of establishment in a Member State.

Article 32(1)(a) and (b), security of processing: engaged by H2, M1 and M2.

Article 35, impact assessment: open question in H3. Processing the health-adjacent signals of a minor is a case the article is written for.

ePrivacy Directive Art. 5(3): engaged by C1, because storing or reading information on terminal equipment requires consent unless strictly necessary.

Consumer Protection & Platform Disclosures

The Google Play listing rates the app PEGI 3 with in-app purchases. The rating addresses the content shown to the account holder and does not describe the processing of data about the monitored infant. No further Play Data Safety statement was read for this report, and none is asserted.

Regulatory & Legal Landscape

The framework applied is the GDPR with Article 27 for a controller outside the Union, together with Article 5(3) of the ePrivacy Directive for terminal equipment. The operator is established in Taiwan and offers its product to EU households, which brings Article 3(2) GDPR into play. No obligation under NIS2 or the AI Act is asserted for this operator, because its sector and size classification has not been established.

The competent authority for an Austrian initiated matter is the Österreichische Datenschutzbehörde (dsb@dsb.gv.at). The European Data Protection Supervisor (edps@edps.europa.eu) is in copy of the notice under the standing practice of the programme. The disclosure follows ISO/IEC 29147 and Art. 17 StGG.

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 from the published package. All values are given in full.

```
Package            com.getcubo.app
Version            2.27.0 (versionCode 2492), analysed 2026-08-22
base.apk SHA-256   302ac3487a7ab15b0930ecba5ad81826a8dfe422fedc406e465a6d93fb45a085
XAPK SHA-256       f3223e7546ff0a0c4033243c684bca87aa39193872fee2b70b5c6040ca0e1173
Signing cert       59:AB:B9:4E:E4:72:28:09:5E:ED:A3:B7:EC:08:BA:65:09:D8:94:ED:4B:BB
    :27:D2:22:FA:99:29:4A:5A:71:C3

Firebase project   cubo-smart-baby-camera
google_api_key     AIzaSyARGu__5GvluNV0zCkNHdqQhgMw7O58YiM
google_app_id      1:1024118653750:android:f82ad8e3e67f1ad5
gcm_defaultSenderId 1024118653750
Storage bucket     cubo-smart-baby-camera.appspot.com
Database URL       https://cubo-smart-baby-camera.firebaseio.com
web client id      1024118653750-n1qo0hi2800ah6cmvod2ui6uhkr954i9.apps.
    googleusercontent.com
```

```
C1  AndroidManifest.xml: FirebaseInitProvider (directBootAware=true, initOrder=100),
    ComponentDiscoveryService, AppMeasurement*
C1  CMP search across resources and classes*.dex (9 files): 0 hits
H1  https://us.getcubo.com/pages/privacy-policy, section on the EU representative
H2  res/values/strings.xml: values above
H3  res/values/strings.xml: gdpr_sa_agreement_term_android, com/getcubo/app/v2/
    features/breathing/*
M1  classes.dex, classes5.dex: cloud/yunyun/cubo/camera/endpoint/TutkEndpoint, com/
    tutk/IOTC/*
M2  res/xml/network_security_config.xml: no pin-set
```

Reproduction: obtain com.getcubo.app 2.27.0 from Google Play, check the SHA-256 above, decode the manifest and resources with apktool and read the named files. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-22 Notice REF CUBOAI-2026-R1 to business@cuboai.com, support@cuboai.com and support@getcubo.com, CC DSB and EDPS. Findings C1, H1, H2, H3 in the text, two medium findings summarised, three questions asked, reply requested within 30 days.

2026-10-17 Follow-up from security@rfi-irfos.com to the same addresses, 34 days before the embargo date, with the open findings and the same three questions.

2026-10-18 Ticket reply from the CuboAi support desk under the subject Collaboration, naming KOL and press addresses. No finding or question addressed.

2026-11-15 Final notice from s.kepp@rfi-irfos.com to the same addresses, five days before the embargo date. No reply followed.

2026-11-20 Embargo date, 90 days after delivery of the notice of 22 August 2026. As of 21 November 2026 no further message from CuboAi is on record, and the report is published.

What CuboAi Got Right

Raw video stays on the camera for 18 hours and is then deleted. Only safety event thumbnails reach the cloud, and the policy gives the exact retention and the scope of a thumbnail. A specific Article 9(2)(a) consent step exists for breathing and sleep analysis, in the app and in the policy. Processors are named, ThroughTek included, with a link to its policy. The network security configuration denies cleartext traffic globally with no exception. The assetlinks.json matches the real signing certificate. ThroughTek AuthKey error codes are present, which points to the newer authentication. No background location permission is requested, and the Danger Zone is a camera-relative zone and not GPS tracking. No ad mediation stack and no PRC or sanctioned-jurisdiction SDK was found in the nine dex files. allowBackup is false and targetSdkVersion is 35.

Residual Risk & Recommendations

Open at the date of publication: all six items, with no written position from the operator. Items that only the operator can close are the consent gate in C1, the representative in H1, the Security Rules and key restrictions in H2, the impact assessment in H3 and the SDK facts in M1.

Recommendations: gate Firebase Analytics and Crashlytics behind a recorded consent decision for paying and non-paying households alike, appoint a representative established in a Member State, restrict the Firebase key by package, certificate and API scope and enforce App Check for the database and the bucket, publish the Article 35 outcome for sleep and breathing analysis, state the ThroughTek SDK version and AuthKey enforcement, and add a pin-set for operator-controlled hosts.

This report is published after the embargo date. Statements are limited to the package and to the public documents named above, and every item the package cannot show is marked UNVERIFIED.

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