Security & Privacy Disclosure, Final Report

AirDroid Parental Control (com.sand.airdroidkidp)

A privacy policy that omits camera snapshots, screen snapshots, SMS monitoring and a nudity classifier over children's photos, which the parent app already ships, and no reply since the notice.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. NO REPLY AS OF 21 NOVEMBER 2026.

Target	SAND STUDIO PTE. LTD., AirDroid Parental Control (parent app)
Version Audited	2.7.7.0 / versionCode 20707000 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	8: 2 High, 5 Medium, 1 Low (R1 labels reassessed, see status table)
Status	NO REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`a49d8aecdca30dcb5e47b3eeb3dd596ce14f329483662433704f38c40de0465f`

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 5

4 Architecture & Data Flow 6

5 Engagement Summary 6

6 Findings 7

6.1 C1: The privacy policy lists four data categories collected from a child's device, while the parent app ships working screens for scheduled camera snapshots, scheduled screen snapshots, SMS and call log monitoring and a nudity classifier over the photo library . . . 7

6.2 C2: A Firebase and Google API key for the project airdroid-parent is hardcoded in every distributed copy of the parent app . . . 8

6.3 H1: The One-Way Audio screen has a Record and save control that the Play listing does not mention . . . 9

6.4 H2: Calls and SMS monitoring covers the call log and message content of people who never installed the app . . . 10

6.5 H3: Cleartext exceptions for four Chinese domains, declared Alibaba and Umeng push components, a parallel Chinese consent flow and Hong Kong governing law point to a Greater China engineering and legal chassis . . . 11

6.6 H4: Automated nudity and content classification of a minor's photos and chats sits next to a policy statement that no sensitive information is processed . . . 13

6.7 M1: Geolocation retention is undefined and the retention sentence for notification data names the wrong data category . . . 14

6.8 M2: The Play listing names a Contacts permission that the manifest does not request . . . 14

7 Impact Analysis 15

8 The Complete Chain 15

9 Child Protection 16

10 Data Protection: Article by Article 16

11 Platform Accountability & DSA 17

12 Regulatory & Legal Landscape 17

13 Indicators of Compromise & Reproducible Evidence 18

14 Disclosure Timeline & Outcome 19

15 What Was Done Well 19

16 Residual Risk & Recommendations 19

Executive Summary

AirDroid Parental Control is the parent app of a child monitoring product from SAND STUDIO PTE. LTD. in Singapore. It has more than 10 million installs on Google Play. The companion app AirDroid Kids runs on the child's device and was not analysed. On 23 August 2026 RFI-IRFOS sent a notice with REF AIRDROIDPARENTAL-2026-R1 to dpo@airdroid.com and support@airdroid.com with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 2.7.7.0 shows that section 2.2.3.2 of the operator's privacy policy lists four categories collected from a child's device, while the parent app ships working screens for scheduled front and rear camera snapshots, scheduled screen snapshots, SMS and call log monitoring and a nudity classifier over the photo library (C1). The classifiers sit next to a policy sentence that no sensitive information is processed (H4). The One-Way Audio screen has a record and save control that the store listing does not mention (H1). Call log and SMS monitoring reaches people who never installed the app (H2). Cleartext exceptions for four Chinese domains, dead Alibaba and Umeng push entries, a parallel Chinese consent flow and Hong Kong governing law point to a Greater China engineering and legal chassis, without showing a data flow (H3). A Firebase key is hardcoded (C2). Two policy and listing mismatches complete the list (M1, M2).

A reassessment by CVSS v4.0 band puts two findings at High, five at Medium and one at Low. The Critical labels of C1 and C2 of 23 August 2026 move to High and Medium. The High labels of H1, H2 and H3 move to Medium. Each change is stated in the status table with its reason. The app is also honest on one point that matters for children: it warns the parent that live screen mirroring shows a recording icon on the child's screen, and it has no hidden or stealth mode.

The operator did not reply to the notice of 23 August 2026 or to the follow-ups of 12 September 2026 and 17 October 2026. This report is published on the embargo date of 21 November 2026 and records the state of the correspondence on 21 November 2026.

Scope: Root level code analysis of the Google Play release 2.7.7.0 (versionCode 20707000) of the parent app, obtained from the APKPure mirror as an XAPK bundle and checked against the package name, developer and version on the live Google Play listing. Work done: manifest, resource and string decode with apktool without source decode, a network security configuration read, and string-pool extraction across all 14 classes dex files with a targeted search for named classes and consent platforms. The live privacy policy at webparent.airdroid.com/privacy.html, the Terms of Service at webparent.airdroid.com/terms.html and the Play listing were read on 23 August 2026 and are treated as primary evidence next to the package. The app was not installed, no account was created, no operator server was called and no traffic was captured. No bytecode control-flow pass and no dynamic instrumentation were done. The companion app AirDroid Kids is a separate package that was not downloaded, so every statement about what it executes rests on the parent app's strings or on the operator's policy. Findings that depend on runtime behaviour are marked as such.

ID	Severity	Title
C1	HIGH	The privacy policy lists four data categories collected from a child's device, while the parent app ships working screens for scheduled camera snapshots, scheduled screen snapshots, SMS and call log monitoring and a nudity classifier over the photo library
C2	MEDIUM	A Firebase and Google API key for the project airdroid-parent is hardcoded in every distributed copy of the parent app
H1	MEDIUM	The One-Way Audio screen has a Record and save control that the Play listing does not mention
H2	MEDIUM	Calls and SMS monitoring covers the call log and message content of people who never installed the app
H3	MEDIUM	Cleartext exceptions for four Chinese domains, declared Alibaba and Umeng push components, a parallel Chinese consent flow and Hong Kong governing law point to a Greater China engineering and legal chassis
H4	HIGH	Automated nudity and content classification of a minor's photos and chats sits next to a policy statement that no sensitive information is processed
M1	MEDIUM	Geolocation retention is undefined and the retention sentence for notification data names the wrong data category
M2	LOW	The Play listing names a Contacts permission that the manifest does not request

ID	Disclosed	This report	State on 14 November 2026

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. Evidence is policy text and file content. Companion app not analysed.
C2	CRITICAL	MEDIUM	No reply. Key restrictions and database rules not tested.
H1	HIGH	MEDIUM	No reply. Policy discloses recording. Listing omits it.
H2	HIGH	MEDIUM	No reply. Capture side not analysed.
H3	HIGH	MEDIUM	No reply. Transfer to China or Hong Kong not shown.
H4	HIGH	HIGH	No reply. Classifier location and storage not analysed.
M1	Not in notice	MEDIUM	Not in notice. Policy text only.
M2	Not in notice	LOW	Not in notice.

The notice of 23 August 2026 labelled C1 and C2 as Critical and H1 to H4 as High, and did not include M1 and M2. This report uses the CVSS v4.0 band of each finding. C1 and H4 stay High through a blast-radius escalation that the finding states. A downgrade is made only where the evidence in the package or in the operator's documents does not carry the earlier label.

Subject & Operator Analysis

The controller named in the Terms of Service is SAND STUDIO PTE. LTD., Unit 30-15, Level 30, Singapore Land Tower, No. 50 Raffles Pl, Singapore 048623. The Terms of Service designate Hong Kong law and arbitration at the Hong Kong International Arbitration Centre. The contacts are dpo@airdroid.com for data protection, confirmed in the live privacy policy, and support@airdroid.com, confirmed on the Play listing. No press contact was found. The Play listing shows 10M+ downloads, 4.4 stars from 153K reviews, the content rating PEGI 3 with in-app purchases, and a paid subscription with a 3 day trial and monthly or annual renewal.

No Article 27 representative in the Union appears in the privacy policy or the Terms of Service retrieved on 23 August 2026. The operator has no identified main establishment in the Union, so the one-stop-shop mechanism does not apply and the Austrian Datenschutzbehörde can receive complaints directly.

Two apps work together. AirDroid Parental Control (com.sand.airdroidkidp) is the parent or controller app and every activity in its manifest is named Parent*. AirDroid Kids is installed on the child's device and holds the sensor, notification and accessibility grants. The operator's privacy policy confirms this split, and says that a child who sets up the companion app first

requests a binding code from the parent app.

Architecture & Data Flow

The parent app is a native Android app with 14 classes dex files of about 61 MB, minSdk 26 and targetSdk 35. It declares no NotificationListenerService, no MediaProjection use and no AccessibilityService, because those run in the companion app. Its own string resources list the capabilities and permission prompts of the companion app, which is how the camera, screen, message and photo features of this report are known.

The backend side is only partly visible. The Firebase project airdroid-parent with a Realtime Database and a storage bucket is named in the resources (C2). The network security configuration forbids cleartext by default and allows it for seven named hosts (H3). Firebase Analytics, Crashlytics and Sessions are present in the manifest with automatic messaging initialisation enabled, and no FirebaseInitProvider pattern before consent was found, so the strongest form of that finding is not claimed. The Facebook SDK is present with automatic initialisation, automatic event logging and advertiser identifier collection all switched off. No advertising mediation SDK was found. The permissions ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID are declared and their purpose is not disclosed. No ACCESS_BACKGROUND_LOCATION is declared, so continuous tracking works through a foreground service or periodic sync. The data model behind the calls was not observed.

Engagement Summary

The notice REF AIRDROIDPARENTAL-2026-R1 was sent on 23 August 2026 at 12:04 UTC from rfi.irfos@gmail.com to dpo@airdroid.com and support@airdroid.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried six findings, a statement of what the product does well and three questions, and set the embargo date of 21 November 2026. A follow-up of 12 September 2026 restated the findings and asked the three questions with an answer date of 19 September 2026. A second follow-up of 17 October 2026 came from security@rfi-irfos.com, announced 35 days to publication, listed five findings as still open and repeated the three questions. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: The privacy policy lists four data categories collected from a child’s device, while the parent app ships working screens for scheduled camera snapshots, scheduled screen snapshots, SMS and call log monitoring and a nudity classifier over the photo library

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B), disclosed as CRITICAL on 23 August 2026, rated HIGH by blast-radius escalation

Section 2.2.3.2 of the privacy policy at webparent.airdroid.com/privacy.html, read on 23 August 2026, lists exactly four categories collected regarding child users of AirDroid Kids: geolocation, the sound around the child’s device, device usage statistics and notification data. The file res/values/strings.xml of version 2.7.7.0 holds complete user interface strings for four further capabilities: scheduled front and rear camera snapshots kept in a retrievable album, scheduled screen snapshots kept the same way, SMS keyword detection with a full call log, and an automated scan of new photos for nudity or adult material. The strings belong to the parent app and describe features that the companion app AirDroid Kids executes on the child’s device. That companion app was not analysed. Where the results are stored or uploaded is therefore UNVERIFIED, and whether a scheduled snapshot shows an indicator on the child’s device was not determined. RFI-IRFOS blast-radius escalation: raised from MEDIUM/5.1 to HIGH because the omitted categories are camera, screen, message and photo content of children, the parent app has more than 10 million installs, and the policy section is the only document that tells a parent what the product collects.

```
<string name="Device_Snapshot_Camera_Timed">Scheduled Camera Snapshot</string>
<string name="Device_Snapshot_Front_Camera">Front-facing Camera</string>
<string name="Device_Snapshot_Rear_Camera">Rear-facing Camera</string>
<string name="Device_Snapshot_Album">Snapshots</string>
<string name="Device_Snapshot_Delete_All_Camera_Confirm">Snapshots cannot be recovered
     once deleted. Are you sure you want to delete all camera snapshots?</string>
<string name="Device_Snapshot_Screen_Timed">Scheduled Screen Snapshots</string>
<string name="Device_Snapshot_Delete_All_Screen_Confirm">Snapshots cannot be recovered
     once deleted. Are you sure you want to delete all screen snapshots?</string>
<string name="Parent_Communicate_Safe_Title">Calls &amp;amp; SMS Monitoring</string>
<string name="Parent_Communicate_SMS_Detect">SMS Keyword Detection</string>
<string name="Parent_Communicate_SMS_Detect_History">SMS Detection Records</string>
<string name="Kid_NSFW_title">Inappropriate Image Detection</string>
<string name="Kid_NSFW_description">Automatically scans new photos in Photos to
    identify inappropriate content, such as nudity or adult material.</string>
```

```
Privacy policy section 2.2.3.2, complete list for child users of AirDroid Kids:
Geolocation
Listen to the sound around the child's device
Access to the device usage statistics
Access to notification data
```

The notice of 23 August 2026 described the camera capture as silent. The package shows

scheduled capture and a persistent album. It does not show whether the child's device displays an indicator for it, so this report does not use the word silent.

Impact: A parent who reads the stated list of what AirDroid collects from the child's device cannot learn that the product offers scheduled front and rear camera snapshots, scheduled screen snapshots held in a retrievable album, SMS content and call log monitoring, or an automated scan of new photos for nudity. The child, whose camera, screen, messages and photos these features address, never sees the policy. The people affected are the children whose parents install AirDroid Kids, and the policy itself defines a child as a person under 16 for users in the Union. The policy is the document a parent or a regulator reads to learn what is processed, and for these four capabilities it says nothing.

Fix: Add the four capabilities to section 2.2.3.2 with the purpose, the legal basis and the retention period of each, or remove the capabilities from the product. State in the policy where snapshots and classifier results are stored.

C2: A Firebase and Google API key for the project airdroid-parent is hardcoded in every distributed copy of the parent app

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as CRITICAL on 23 August 2026

The file res/values/strings.xml holds the key as google_api_key and again as google_crash_reporting_api_key, together with the Firebase Realtime Database URL, the storage bucket and the project identifiers. The same file holds a Google Maps key and a Facebook application identifier with client token. Google documents such keys as identifiers and not as secrets. The exposure is availability, because anyone can extract the key and spend the project's API quota. The project plausibly serves a child monitoring product, so the security rules of the Realtime Database and the bucket matter. They were not tested, no call with the key was made, and the key restrictions are not visible from the package.

```
google_api_key                  AIzaSyDsS489ncgxeQ9nat2Y3WdvEXEGvp1g8a4
google_crash_reporting_api_key  AIzaSyDsS489ncgxeQ9nat2Y3WdvEXEGvp1g8a4
firebase_database_url           https://airdroid-parent.firebaseio.com
google_app_id                   1:94870192826:android:9bba6f1ea4bd818385b883
project_id                      airdroid-parent
google_storage_bucket           airdroid-parent.appspot.com
default_web_client_id           94870192826-sbm1c7kjvpbh99614hjploph0an1s83n.apps.
    googleusercontent.com
gcm_defaultSenderId             94870192826
google_maps_key                 AIzaSyBwYFVxygS2ZyW__l1drqRVAe2-nMVBW-4
facebook_app_id                 167747143358481
facebook_client_token           1173db067b43cc332a08d0a2d6d5ff90
```

The same file records push application identifiers for Huawei, Honor and Vivo. The source file of this analysis does not record their values, so the full values are missing from this report and are not shortened here.

Impact: Anyone can read the key from the package in under a minute. Exhausting the quota of the project could slow or stop the functions that depend on it, such as push messages to parents. Whether the project holds location, notification or snapshot data of children is not shown, and the state of its security rules is unknown.

Fix: Restrict the key by package name and signing certificate, review the Realtime Database and bucket rules, and move any privileged call to a server side component.

H1: The One-Way Audio screen has a Record and save control that the Play listing does not mention

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B), disclosed as HIGH on 23 August 2026

The Play listing, read on 23 August 2026, describes the feature as remotely listening to surrounding sounds from the child's device in emergencies, and says that all audio data is saved locally on parent devices with no server storage. The parent app strings show a Record control, a Stop recording control and a line saved to, so a parent can create a durable audio file of the child's surroundings. The operator's privacy policy discloses the choice to record. The gap sits in the store listing, which a buyer reads first. The no server storage claim concerns servers only. The file on the parent's phone is real personal data about the child's environment and about anyone whose voice is picked up.

```
<string name="Parent_Device_Listening_Title">One-Way Audio</string>
<string name="Parent_Device_Listening_Record">Record</string>
<string name="Parent_Device_Listening_End_Record">Stop recording</string>
<string name="Parent_Device_Listening_Recording">Recording:</string>
<string name="Parent_Device_Listening_Save">saved to:</string>
```

```
"Private Ambient Sound Monitoring - Remotely listen to surrounding sounds from your
    child's device in emergencies. All audio data saves locally on parent devices with
     no server storage for maximum privacy and security."
```

```
"you as a parent can choose to listen live to your child's device's surroundings, or
    choose to record these surroundings."
```

Impact: A buyer who reads the store listing learns of passive listening in emergencies. The product also lets a parent record the surroundings of a child and keep the file. The recording can capture other children, family members and visitors near the device. The operator's policy mentions the recording, so the information exists but not where the purchase decision is made.

Fix: Describe the record function in the Play listing and the in-app introduction of the feature, and state who can access a saved file.

H2: Calls and SMS monitoring covers the call log and message content of people who never installed the app

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

The parent app has a Calls and SMS Monitoring area with incoming and outgoing call lists, SMS keyword detection and SMS detection records, and a message that tells the parent when SMS permission is missing on the child's device. Every number that calls or texts the monitored child enters the feature: relatives, classmates, teachers, doctors and helplines. These people never saw a consent screen, a policy or a store listing. The capture runs in the companion app on the child's device. That app was not analysed, so whether message content reaches the operator's servers or stays on the parent's device is UNVERIFIED.

```
<string name="Parent_Communicate_Safe_Title">Calls &amp;amp; SMS Monitoring</string>
<string name="Parent_Communicate_Call_Log_Incoming">Incoming</string>
<string name="Parent_Communicate_Call_Log_Outgoing">Outgoing</string>
<string name="Parent_Communicate_SMS_Detect">SMS Keyword Detection</string>
<string name="Parent_Communicate_SMS_Detect_History">SMS Detection Records</string>
<string name="ad_permission_calllog">Call History</string>
<string name="Parent_Permission_SMS_No_Auth">"You haven't granted permission to SMS on
     the child's device."</string>
```

Impact: Third parties who contact a monitored child are recorded as a side effect of monitoring one person. Their information obligation under Art. 14 is structurally hard to meet, because the operator has no contact with them. The child's own correspondence, including messages to a doctor or a helpline, passes through the same feature.

Fix: State in the policy how call log and SMS data of third parties is handled, restrict retention to what the keyword feature needs, and document the basis for the processing.

H3: Cleartext exceptions for four Chinese domains, declared Alibaba and Umeng push components, a parallel Chinese consent flow and Hong Kong governing law point to a Greater China engineering and legal chassis

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

Five artifacts point the same way. The network security configuration permits cleartext HTTP for amap.com, 4399.com, baidu.com and iqiyi.com, for airdroid.com and for two private addresses, while the base configuration forbids cleartext. The manifest declares receivers and a service for the Alibaba Taobao AGOO push SDK and the Umeng push SDK, and a search of all 14 classes dex files finds none of the three class names, so these entries are dead in this build. The string resources carry a parallel Chinese consent flow with its own children's privacy policy next to the global one. The Terms of Service designate Hong Kong law and arbitration at the Hong Kong International Arbitration Centre, while the registered entity is SAND STUDIO PTE. LTD. in Singapore. The privacy policy states in section 9 that data of the user and the child can be transferred to anywhere in the world and names no transfer mechanism. None of this shows that data of a user in the Union reaches mainland China or Hong Kong in the global build. The dead push components argue against it for push messages, and the cleartext exceptions and the blanket transfer clause keep the question open. A comparison with FlashGet Kids found no shared backend between the two products.

```
<base-config cleartextTrafficPermitted="false" />
<domain-config cleartextTrafficPermitted="true">
  <domain includeSubdomains="true">192.168.40.201</domain>
  <domain includeSubdomains="true">192.168.40.37</domain>
  <domain includeSubdomains="true">amap.com</domain>
  <domain includeSubdomains="true">4399.com</domain>
  <domain includeSubdomains="true">baidu.com</domain>
  <domain includeSubdomains="true">iqiyi.com</domain>
  <domain includeSubdomains="true">airdroid.com</domain>
</domain-config>
```

```
com.taobao.agoo.AgooCommondReceiver
com.sand.airdroidkidp.domain.manager.umeng.MfrMzMessageReceiver
com.sand.airdroidkidp.domain.services.ParentUmengPushMessageService
```

```
Parent_Privacy_Checkbox1_CN      I have read and agree to the Children's Privacy
    Policy (cn_childprivacy)
Parent_Privacy_Checkbox1_Global  I have read and agree to the Terms of Service (eula)
    and the Privacy Policy (privacy)
```

```
Terms of Service, governing law:  Hong Kong law (excluding conflict-of-laws rules)
Dispute forum:  Hong Kong International Arbitration Centre
Registered entity:  SAND STUDIO PTE. LTD., Unit 30-15, Level 30, Singapore Land Tower,
     No. 50 Raffles Pl, Singapore 048623
Privacy policy section 9:  "Your Service is global by nature and Your and Your child's
     data can therefore be transferred to anywhere in the world"
```

Impact: Users and the parents who consent for their children cannot tell from the operator's documents which countries process the data of a child, and no transfer mechanism is named. The legal and engineering artifacts make it reasonable to ask the question. They do not answer it. The Hong Kong forum clause is a practical obstacle for a parent in the Union who wants redress.

Fix: Name the processors and their countries, name the Art. 46 mechanism and the transfer impact assessment, remove dead components and the four unrelated cleartext domains, and name an Art. 27 representative.

H4: Automated nudity and content classification of a minor's photos and chats sits next to a policy statement that no sensitive information is processed

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as HIGH on 23 August 2026, rated HIGH by blast-radius escalation

Section 2.2.7 of the privacy policy states that the operator does not collect or process any sensitive information, such as information related to racial or ethnic origin, political opinions, religious beliefs, physical or mental health, or crime. The parent app strings describe three classifiers: an inappropriate image detection that scans new photos for nudity or adult material, a social content detection that scans for flagged keywords to alert to cyberbullying and inappropriate interactions, and a potential risk detection that spots behaviours such as late-night usage or unusual searches. Each reads the substance of a minor's private images, conversations or behaviour and produces a derived label that is more sensitive than the sentence in section 2.2.7 allows for. Where the classifiers run, on the child's device or in a cloud service, and where the labels are stored, was not examined. None of the three derived labels appears in the policy's list of collected data. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the classifiers process private images and conversations of children at the scale of a product with more than 10 million installs, and the operator's own policy denies processing sensitive information.

```
Privacy policy section 2.2.7:
"Sensitive Information. We do not collect or process any sensitive information, such
    as information related to the racial or ethnic origin, political opinions,
    religious beliefs, physical or mental health or condition, crime or court records,
     etc."
```

```
<string name="Kid_NSFW_title">Inappropriate Image Detection</string>
<string name="Kid_NSFW_description">Automatically scans new photos in Photos to
    identify inappropriate content, such as nudity or adult material.</string>
<string name="Parent_Keyword_Detect">Social Content Detection</string>
<string name="Parent_TourMode_SocialDetect_Body">Scan for flagged keywords and alert
    you to cyberbullying, inappropriate interactions, or other potential risks.</
    string>
<string name="kid_ai_risk_detection_title">Potential Risk Detection</string>
<string name="kid_ai_risk_detection_description">Spots behaviors like late-night usage
     or unusual searches to keep risks at bay.</string>
```

Impact: The product runs a nudity classifier over the photo library of a child and a keyword scan over the child's chats, and the policy tells parents and regulators that no sensitive information is processed. A derived label such as flagged for nudity can be more sensitive than any raw value it comes from. The affected group is the children whose parents enable these features, and the classifier handles images that can themselves be intimate images of a minor. A data protection impact assessment for this processing was asked for in the notice and has not been shown.

Fix: Correct section 2.2.7, list the three derived labels in the data inventory, state where each classifier runs and how long each label is kept, and publish or supply the data protection

impact assessment to the supervisory authority.

M1: Geolocation retention is undefined and the retention sentence for notification data names the wrong data category

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.3 (CVSS-B), first stated in this report

Section 2.2.3.2 of the privacy policy says for geolocation that the operator only stores it as long as it is reasonable to provide the Service. For notification data the same section says that the operator only stores the geolocation data as long as 48 hours and then deletes the notification data related to the profile. The controlling sentence for notification data therefore names geolocation. Continuous location of a child, marketed with geofence alerts and route history, has no retention period that a person or a regulator can test. A reader cannot tell whether location also carries a 48 hour cap or is kept for the lifetime of the account.

```
Geolocation: ... We only store the geolocation data as long as it is reasonable to
    provide the Service.
Access to notification data: ... We only store the geolocation data as long as 48
    hours, and then we delete the notification data related with your profile in the '
    AirDroid Parental Control' application.
```

Impact: Parents and children cannot hold the operator to a stated retention period for location history or for notification data. The question is a drafting defect with a legal consequence, because Art. 13(2)(a) requires the period or the criteria.

Fix: State a concrete retention period for location history and correct the notification sentence.

M2: The Play listing names a Contacts permission that the manifest does not request

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

The Required Permissions section of the Play listing says Contacts: Assist in GPS safety contact setup. The manifest of version 2.7.7.0 declares no READ_CONTACTS, WRITE_CONTACTS or GET_ACCOUNTS permission. The most plausible cause is stale listing copy from an earlier build or a shared template. The mismatch is a representation to prospective installers that does not match the build.

```
Play listing, Required Permissions:  "Contacts: Assist in GPS safety contact setup"
AndroidManifest.xml:  no READ_CONTACTS, WRITE_CONTACTS or GET_ACCOUNTS
```

Impact: A prospective installer is told to expect a permission that the build does not use. The effect on data is none.

Fix: Correct the listing.

Impact Analysis

The people affected are children whose parents run AirDroid Kids on the child's phone, and the parents who consent for them. The policy defines a child as a person under 16 for users in the Union. Further people are the callers and message partners of the child, and anyone whose voice is picked up near the child's device.

The weight of the case sits on the gap between what the policy says and what the product does. A parent reading section 2.2.3.2 learns of four data categories and is not told of camera snapshots, screen snapshots, SMS and call monitoring or the nudity classifier (C1). The same policy says that no sensitive information is processed while the classifiers read the child's photos and chats (H4). The recording function of the audio feature appears in the policy and not in the store listing (H1).

What the package shows is labelled capability, policy text and file content. No snapshot, message, photo or audio value was observed leaving a device, and the report asserts no such flow.

The Complete Chain

Step 1, purchase: a parent finds the app on Google Play, rated PEGI 3, with a listing that describes passive listening in emergencies and a required permission that the build does not use (H1, M2).

Step 2, consent: the parent accepts the Terms of Service and the privacy policy. The policy lists four categories collected from the child's device and says no sensitive information is processed (C1, H4). A Chinese language consent flow with its own children's policy exists in the same build (H3).

Step 3, pairing: the parent installs AirDroid Kids on the child's device with a binding code. The child never sees the parent app, the listing or the policy.

Step 4, use: the parent can schedule front and rear camera snapshots and screen snapshots into an album, record the child's surroundings, read call and SMS records of the child and anyone who contacts the child, and receive the results of a nudity classifier over new photos (C1, H1, H2, H4).

Step 5, back end: a Firebase project and a storage bucket serve the product, the key sits in every copy of the package (C2), and the retention of location history is undefined (M1).

Step 6, rights: the policy allows transfer to anywhere in the world, names no mechanism and no representative in the Union, and the Terms of Service send disputes to Hong Kong (H3).

Child Protection

The group at the centre of this case is children who are monitored by a parent through AirDroid Kids. They have no view of the parent app, the Play listing or the policy. The Play rating of PEGI 3 describes the content seen by the adult who installs the parent app. It says nothing about the processing of the child, who is the actual data subject. This is a structural mismatch of the rating scheme and this report draws no conclusion from the number itself.

Two protections exist and are credited. First, the app warns the parent that live screen mirroring shows a recording icon at the top of the child's screen, two Play reviewers report the same operating system indicators, and the operator's public reply says that the operating system shows them and the app cannot hide them. No string, activity or setting for a stealth, invisible or hide icon mode exists in the parent app. Second, a verifiable parental consent flow exists for the United States, with an email confirmation and a revocation path, for children under 13.

The open points are three. Whether a scheduled camera or screen snapshot triggers the same indicator on the child's device was not determined. The policy defines a child as under 16 for users in the Union and describes no verification mechanism that is distinct from the United States flow. Austria sets the age of digital consent at 14 in § 4 Abs. 4 DSG, and the operator's policy does not mention it.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, H1 and H4.

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

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

Article 5(2), accountability: engaged by C1.

Article 6(1): engaged by H2 for third parties.

Article 8, children: the policy defines a child as under 16 for users in the Union and describes no distinct verification mechanism. The point is raised in the notice as question 3 of the second part and is not rated as a finding.

Article 9: engaged by H1 for ambient audio and by H4 for the classifiers. No processing of special categories by the operator is asserted. The engagement is the denial in section 2.2.7 and the content that the classifiers read.

Article 12 and Article 13(1)(c): engaged by C1 and H1. Article 13(1)(f) is engaged by H3 and Article 13(2)(a) by M1. Article 14 is engaged by C1 for the child and by H2 for callers and message partners.

Article 25: engaged by C2.

Article 27: no representative in the Union was found in the policy or the Terms of Service on 23 August 2026.

Article 32(1)(b): engaged by C2.

Article 35: engaged by H4 for automated classification of a minor's images and conversations. No assessment was shown.

Articles 44 and 46: engaged by H3 as an open question.

Platform Accountability & DSA

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

The Play listing, read on 23 August 2026, describes the audio feature without its record function (H1) and names a Contacts permission that the manifest does not request (M2). The Data Safety section of the listing was not recorded in the source file of this analysis and is not assessed in this report.

Regulatory & Legal Landscape

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

Infringements of Art. 5, 6, 7 and 9, of Art. 12 to 22 and of Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 25, 27 and 32 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82. Art. 5(3) of the ePrivacy Directive covers access to information on the user’s device. The Terms of Service choose Hong Kong law and arbitration. A choice of foreign law and forum between operator and parent does not limit the rights of a data subject under the GDPR.

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

Indicators of Compromise & Reproducible Evidence

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

```
Package            com.sand.airdroidkidp
Version            2.7.7.0 (versionCode 20707000), minSdk 26, targetSdk 35, compileSdk
     36
Base APK size      109.5 MB
Base APK SHA-256   a49d8aecdca30dcb5e47b3eeb3dd596ce14f329483662433704f38c40de0465f
XAPK SHA-256       10f20dd68ea5cb2ac9bc25c55c325f3fa06cc52772bd6581f41abad8c5f449df
Audit device       none, the app was not installed
Acquisition        APKPure mirror, checked against the Google Play listing, 2026-08-23
```

```
google_api_key                  AIzaSyDsS489ncgxeQ9nat2Y3WdvEXEGvp1g8a4
google_crash_reporting_api_key  AIzaSyDsS489ncgxeQ9nat2Y3WdvEXEGvp1g8a4
google_maps_key                 AIzaSyBwYFVxygS2ZyW__l1drqRVAe2-nMVBW-4
firebase_database_url           https://airdroid-parent.firebaseio.com
google_app_id                   1:94870192826:android:9bba6f1ea4bd818385b883
project_id                      airdroid-parent
google_storage_bucket           airdroid-parent.appspot.com
default_web_client_id           94870192826-sbm1c7kjvpbh99614hjploph0an1s83n.apps.
    googleusercontent.com
gcm_defaultSenderId             94870192826
facebook_app_id                 167747143358481
facebook_client_token           1173db067b43cc332a08d0a2d6d5ff90
Huawei, Honor and Vivo push IDs  full values not recorded in the source file
Cleartext hosts                 192.168.40.201, 192.168.40.37, amap.com, 4399.com,
    baidu.com, iqiyi.com, airdroid.com
Policy and terms                https://webparent.airdroid.com/privacy.html, https://
    webparent.airdroid.com/terms.html
Contacts                        dpo@airdroid.com, support@airdroid.com
```

```
C1  res/values/strings.xml (Device_Snapshot_*, Parent_Communicate_*, Kid_NSFW_*),
    privacy policy section 2.2.3.2
C2  res/values/strings.xml (google_api_key and related values)
H1  res/values/strings.xml (Parent_Device_Listening_*), Play listing, privacy policy
H2  res/values/strings.xml (Parent_Communicate_*, ad_permission_calllog,
    Parent_Permission_SMS_No_Auth)
H3  res/xml/network_security_config.xml, AndroidManifest.xml (AGOO and Umeng entries),
     classes*.dex, res/values/strings.xml (Parent_Privacy_Checkbox1_*), Terms of
    Service, privacy policy section 9
H4  privacy policy section 2.2.7, res/values/strings.xml (Kid_NSFW_*,
    Parent_Keyword_Detect, kid_ai_risk_detection_*)
M1  privacy policy section 2.2.3.2
M2  Play listing, AndroidManifest.xml
```

Reproduction: obtain com.sand.airdroidkidp 2.7.7.0 (20707000), check the SHA-256 value above, decode manifest and resources with apktool without source decode, search the 14 classes dex files for the three named push classes, and read the privacy policy and Terms of Service at the addresses above. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF AIRDROIDPARENTAL-2026-R1 at 12:04 UTC to dpo@airdroid.com and support@airdroid.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Six findings, three questions, embargo date 21 November 2026.

2026-09-12 Follow-up at 16:46 UTC to both addresses. It restated the open findings and asked the three questions, on the omitted data categories, the impact assessment for the nudity classifier and the transfer mechanism with the representative in the Union, with answers due on 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:01 UTC. It announces 35 days to publication, lists five findings as still open and repeats the three questions.

2026-11-14 No reply of any kind and no delivery failure.

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

What Was Done Well

The network security configuration sets cleartext traffic to forbidden by default and scopes the exceptions to a named list. No stealth, invisible or hide icon mode exists in the parent app. The app warns the parent in its own text that live screen mirroring shows a recording icon on the child’s screen. The Facebook SDK has automatic initialisation, automatic event logging and advertiser identifier collection switched off. No advertising mediation SDK was found, which matches the ad-free positioning of the subscription. A verifiable parental consent flow exists for children under 13 in the United States. The policy states that data is not sold or rented and that children’s data is not used for targeted advertising.

Residual Risk & Recommendations

Open at the date of publication: all eight findings. The operator has not replied. The companion app AirDroid Kids remains the largest open question, because it holds the camera, microphone, accessibility and notification grants and executes every capture described here. A final APK diff against version 2.7.7.0 and a fresh reading of the privacy policy and the listing before 21 November 2026 determine the state that the published report records.

Recommendations in order of effect. First, bring section 2.2.3.2 in line with the product and say where snapshots and classifier labels are stored (C1). Second, correct section 2.2.7 and supply the impact assessment for the classifiers (H4). Third, describe the record function in the listing (H1) and state how third party call and message data is handled (H2). Fourth, name processors, countries, the transfer mechanism and a representative in the Union (H3). Fifth, restrict the Firebase key and review the database and bucket rules (C2). Sixth, state concrete retention periods and correct the listing (M1, M2).

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria RFI-IRFOS research focus institute · ZVR 1015608684 ·

GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. Root level code analysis of the published application only. CVSS values

are CVSS v4.0 Base (CVSS-B) and model technical exposure, so transparency findings fit the scale only approximately. Labels above the computed band carry a blast-radius escalation statement in the finding. Final report, published 21 November 2026. REF AIRDROIDPARENTAL-2026-R1.