Security & Privacy Disclosure, Final Report

FlashGet Kids (com.flashget.parentalcontrol)

A parental monitoring app that offers to hide the child app from the child, starts two analytics collectors before any consent screen, and has not replied since the notice.

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

Target	Hongkong FlashGet Network Technology Co., Ltd., FlashGet Kids (parent app)
Version Audited	1.4.1.0 / versionCode 104010008 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	7: 3 High, 4 Medium (R1 labels reassessed, see status table)
Status	NO REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`4b7e2cf8fb73d8143a22f17dd7d871243903e5c2cb5e1f903fc4d2ca13129931`

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 app ships a Disguise App function that installs a disguised child app and hides its icon from the child, while its own consent text warns that concealed surveillance may be a criminal act . . . 7

6.2 C2: Firebase, Tencent Beacon and an advertising and attribution configuration start before any consent screen can render on a paid subscription product, with no consent platform in the package . . . 9

6.3 H1: The Play Data Safety declaration says no data is shared with third parties and lists only device IDs, while the package and the operator's own policy show otherwise . . . 10

6.4 H2: The parent app compiles in device identifier probing for the services of seven phone makers . . . 11

6.5 H3: A Tencent Cloud real-time communication, storage and media AI stack carries the camera, audio and screen monitoring, in tension with the policy statement that audio is not stored on servers . . . 12

6.6 H4: The policy names no representative in the Union and no data protection officer, while it defines children of the Union as a processed category . . . 13

6.7 M1: The network security configuration permits cleartext traffic for the whole app, with a private address entry and no certificate pinning . . . 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

FlashGet Kids is a parental monitoring platform operated by Hongkong FlashGet Network Technology Co., Ltd. in Hong Kong. It has more than 10 million installs on Google Play. This report covers the parent app, com.flashget.parentalcontrol, which is the viewer. The capture of camera, microphone and screen runs in a separate child app, FlashGet Kidsafe, that the parent installs on the child's device from a link and not from Google Play. That child app was not obtained. On 23 August 2026 RFI-IRFOS sent a notice with REF FLASHGETKIDS-2026-R1 to support@flashget.com with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

A root level code analysis of version 1.4.1.0 shows that the parent app ships a Disguise App function and a hide icon function for the child app, while its own consent text warns that illegal surveillance may be a criminal act (C1). Firebase, Tencent Beacon and an open attribution configuration start before any consent screen on a paid product, and no consent platform exists in the package (C2). The Data Safety card says no data is shared with third parties (H1). The app compiles in identifier probing for seven phone makers (H2). A Tencent Cloud real-time communication, storage and media AI stack carries the monitoring, and the policy says audio is not stored on servers (H3). The policy names no representative in the Union and no data protection officer (H4). The network security configuration permits cleartext for the whole app (M1).

A reassessment by CVSS v4.0 band puts two findings at High and five at Medium before that escalation. The Critical labels of C1 and C2 of 23 August 2026 move to High. The High labels of H1 to H4 move to Medium. M1 is held at High by a blast-radius escalation that the finding states. Each change is stated in the status table with its reason. The operator publishes a detailed policy with a COPPA parental consent flow for the United States, states that children's data is not used for targeted advertising, and sets allowBackup to false.

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, and no delivery failure was returned. 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 1.4.1.0 (versionCode 104010008) of the parent app, obtained from the APKPure mirror as an XAPK bundle of 94.7 MB with a base APK of 64,107,967 bytes and an arm64 library split of 35,219,110 bytes. The mirror hash was recomputed on the analysis host and matches the hash stated by the publisher, and package name, developer and version were checked against the live Google Play listing. An earlier mirror was abandoned because its download button led through unrelated pop-ups. Work done: manifest, resource and string decode with apktool without source decode, a network security configuration read, and string extraction across 7 classes dex files and the native library list. Memory constraints on the analysis host ruled out a full code disassembly. The live privacy policy at kids.flashget.com/privacy-policy, the Terms of Service and the Play listing with the Data Safety card 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. The child app FlashGet Kidsafe was not obtained, so every statement about what it executes rests on the parent app strings or on the operator's documents. A comparison with AirDroid Parental Control by string search is recorded in the folder and summarised in H2 and in the architecture section.

ID	Severity	Title
C1	HIGH	The app ships a Disguise App function that installs a disguised child app and hides its icon from the child, while its own consent text warns that concealed surveillance may be a criminal act
C2	HIGH	Firebase, Tencent Beacon and an advertising and attribution configuration start before any consent screen can render on a paid subscription product, with no consent platform in the package
H1	MEDIUM	The Play Data Safety declaration says no data is shared with third parties and lists only device IDs, while the package and the operator’s own policy show otherwise
H2	MEDIUM	The parent app compiles in device identifier probing for the services of seven phone makers
H3	MEDIUM	A Tencent Cloud real-time communication, storage and media AI stack carries the camera, audio and screen monitoring, in tension with the policy statement that audio is not stored on servers
H4	MEDIUM	The policy names no representative in the Union and no data protection officer, while it defines children of the Union as a processed category
M1	HIGH	The network security configuration permits cleartext traffic for the whole app, with a private address entry and no certificate pinning

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	HIGH	No reply. Child app not obtained. Evidence is strings in the parent app.
C2	CRITICAL	HIGH	No reply. Question 2 of the notice unanswered. Data sent at start not observed.
H1	HIGH	MEDIUM	No reply. Question 2 of the follow-ups unanswered. Discrepancy stated, cause unknown.
H2	HIGH	MEDIUM	No reply. Call site not traced.
H3	HIGH	MEDIUM	No reply. Question 3 of the notice unanswered. Routing not captured.
H4	HIGH	MEDIUM	No reply. Question 3 of the notice unanswered. Policy text of 2026-08-23.
M1	Not in notice	HIGH	Not in notice. No cleartext endpoint identified. Held at High by blast-radius escalation.

The notice of 23 August 2026 labelled C1 and C2 as Critical and H1 to H4 as High, and did not include M1. This report uses the CVSS v4.0 band of each finding. C1 and C2 stay High through a blast-radius escalation that the finding states, and M1 is raised to High the same way. 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 privacy policy is Hongkong FlashGet Network Technology Co., Ltd., FLAT 2304, 23/F HO KING, COMMERCIAL CENTRE, 2-16 FA YUEN STREET, MONG KOK KOWLOON, HONG KONG. The Terms of Service designate Hong Kong law and arbitration at the Hong Kong International Arbitration Centre, seated in Hong Kong. The only contact found in the policy and the Terms of Service is support@flashget.com, which the Play listing also names. No dedicated privacy or press address and no data protection officer was found. The Play listing shows more than 10 million downloads, about 111 thousand reviews and a position as the fourth top-grossing app in Parenting.

No Article 27 representative in the Union was found in the policy or the Terms of Service read on 23 August 2026 (H4). 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. FlashGet Kids, com.flashget.parentalcontrol, is the parent app: its application class is ProtectedSandApp, every activity is named Parent*, the launcher icon is parent_ic_launcher and the app label is parent_app_name_simple. It declares no RECORD_AUDIO permission, and the string does not appear in any dex file. The child app, FlashGet Kidsafe, holds the capture logic. The package name of that app was not established.

Architecture & Data Flow

The parent app targets SDK 35 with minimum SDK 24 and has 7 classes dex files. It uses Firebase (Analytics, Crashlytics, RemoteConfig, Messaging), the Tencent stack described in H3, the OAID wrapper library of H2, Google Maps with a hardcoded maps key, and a Facebook SDK with the placeholder values 1234 and 56789, which suggests that collector is inactive in this build. The full value of the maps key is not recorded in the source file of this analysis and is not shortened here.

The monitoring screens of the parent app are remote camera, one-way audio and screen mirroring, which run on the Tencent real-time stack, together with camera snapshots, environment snapshots and screen recording activities. Screen mirroring and the synchronised notifications give the operator sight of every other app the child uses, among them social and messaging apps, so a finding in this product reaches third party services that have no relationship with the operator. The privacy policy says notification content is kept for 48 hours.

The backend side is not visible. Which servers, regions and retention periods apply was not observed, and no traffic was captured. FirebaseRemoteConfig is compiled in, so the operator can change features after installation without a release. No exercised change was traced.

The comparison with AirDroid Parental Control tested the thesis of a shared white-label backend and did not confirm it. AirDroid’s package holds none of FlashGet’s Tencent Cloud modules. The only overlaps are the local storage utility mmkv and the open-source OAID wrapper, which are common tooling.

Engagement Summary

The notice REF FLASHGETKIDS-2026-R1 was sent on 23 August 2026 at 12:04 UTC from rfi.irfos@gmail.com to support@flashget.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried six findings, a statement that the analysed app is the parent component, and three questions, and set the embargo date of 21 November 2026. A follow-up of 12 September 2026 at 16:37 UTC restated three findings and three questions with an answer date of 26 September 2026. A second follow-up of 17 October 2026 at 19:04 UTC came from security@rfi-irfos.com, announced 35 days to publication, listed the open points and repeated the three questions. No inbound message from the operator exists in the mailbox and no delivery failure was returned.

Findings

C1: The app ships a Disguise App function that installs a disguised child app and hides its icon from the child, while its own consent text warns that concealed surveillance may be a criminal act

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 CRITICAL on 23 August 2026, rated HIGH by blast-radius escalation

The file res/values/strings.xml of the parent app holds a complete set of strings for disguising the child app and hiding its icon. The parent is told to tap Disguise App to install a disguised version and hide the real app from the child, and that the icon of the child's app will be hidden after installation. One string warns that leaving the installer on the device may expose the child app. The accessibility step for the child app is written for the disguised name. The same string table holds the operator's consent text for the parent, which states that illegal surveillance and recording activities without lawful authorization may be considered criminal acts. The platform calls for toggling a launcher alias at runtime, getComponentEnabledSetting and setComponentEnabledSetting, appear in the same class set. The child app was not obtained, so how the concealment works and which permissions the disguised app requests are UNVERIFIED. A public Play review dated 25 July 2026 reports that the accessibility setting on the child's phone switches itself off again. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the function hides a monitoring app from a minor who is the data subject of camera, audio, location and notification data, and the app has more than 10 million installs.

```
App Disguised
AppDisguised_Des / AppDisguised_Title
DisguiseApp_Button
DisguiseAppPage_Des: "Tap "Disguise App" to install a disguised version and hide the
    real app from your child."
Disguise Failed / DisguiseFailed_Des / DisguiseFailed_Title
DisguiseStatus_Disguised / DisguiseStatus_NotDisguised
Feature_Title_HideIcon / Feature_Des_HideIcon
kid_hide_icon_page_button / _content / _msg / _off / _on
Download_Popup_HideDescription2: "The icon of the child's app will be hidden after the
     installation."
Installer_Exposure_Warning: "Leaving it installed may expose the child app."
EnableAccessibility_PopUp_Step1Des_Disguised: "[_When granting permissions, find the
    app under its disguised name, ..."
```

```
Kid_TermsConfirmation_Description: "You confirm that as the guardian or legal agent of
     the device, have
installed the App for your child, and agree and authorize our products to obtain the
    data and
information of your child's device. [...] You understand that illegal surveillance and
     recording
activities without lawful authorization may be considered criminal acts and subject to
     legal liability."
```

Concealment of a monitoring app from the monitored person is the trait that separates covert monitoring software from open parental control. Whether a Google Play policy on covert monitoring applies to this feature was not verified in this analysis, and the finding stands on the strings and on Art. 5(1)(a), 12 and 13 of the GDPR.

Impact: The person recorded is a minor, who by design is denied the one signal that would let them know monitoring exists, an app icon. A person cannot exercise a right over data collected by a presence they cannot see. The operator places the legal risk on the parent who taps Agree. The function does not distinguish a parent of a child from any other person who installs the app on someone else's phone, and the Kid_TermsConfirmation text is the only protection the package shows.

Fix: Remove the concealment function, or limit it to a fixed visible indicator on the child's device, and show the child that monitoring is active.

C2: Firebase, Tencent Beacon and an advertising and attribution configuration start before any consent screen can render on a paid subscription product, with no consent platform in the package

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 23 August 2026, rated HIGH by blast-radius escalation

The manifest declares FirebaseInitProvider with init order 100 and direct boot awareness, so Android starts it during application creation, before any activity and before the device is unlocked. The manifest forces firebase_messaging_auto_init_enabled to true. The Privacy Sandbox attribution configuration permits all callers. The manifest declares the permissions AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID. The dex files hold the Firebase classes for Analytics, Crashlytics, RemoteConfig and Messaging and the Tencent Beacon analytics classes. A case-insensitive search of the strings and dex files for onetrust, didomi, usercentrics, iabtcf, consentmanager, cmpsdk, tcf2 and iabconsent returned no match, so no consent platform exists in the package. The manifest also declares a live Play Billing integration, and the strings hold a free trial then paid structure per month, quarter and year, and a PayPal path on the operator's website. Which data the two collectors send at start was not observed. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the app is a paid parental monitoring product, one of the two collectors is run by a company in the PRC, and the app has more than 10 million installs.

```
<provider android:name="com.google.firebase.provider.FirebaseInitProvider"
          android:authorities="com.flashget.parentalcontrol.firebaseinitprovider"
          android:directBootAware="true" android:initOrder="100" android:exported="
    false"/>
<meta-data android:name="firebase_messaging_auto_init_enabled" android:value="true"/>
<property android:name="android.adservices.AD_SERVICES_CONFIG" android:resource="@xml/
    ga_ad_services_config"/>
```

```
<ad-services-config>
    <attribution allowAllToAccess="true" />
</ad-services-config>
```

```
com.google.android.gms.permission.AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_AD_ID
com.android.vending.BILLING
com.google.android.play.billingclient.version = 7.1.1
```

Impact: A parent who pays for this app is tracked by two independent analytics collectors from the moment the process starts, one operated in the United States and one by a company in the PRC, with no consent gate of any kind. The justification of an advertising funded free app does not apply to a product that collects money. The parent app also connects the parent to the child's data, so the start-up processing sits in a product whose subject is a minor.

Fix: Start Firebase, Tencent Beacon and the attribution components only after a consent decision, restrict the attribution configuration to named callers, and document the legal basis for the start-up processing.

H1: The Play Data Safety declaration says no data is shared with third parties and lists only device IDs, while the package and the operator's own policy show otherwise

---

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 Data Safety section of the Play listing, captured on 23 August 2026, says no data is shared with third parties, that the app may collect Device or other IDs, that data is encrypted in transit and that deletion can be requested. The package holds Firebase Analytics, Tencent Beacon analytics, a Google Maps key, the AD_ID and Privacy Sandbox attribution configuration with all callers allowed, a dormant Facebook SDK and the multi-vendor device identifier probing of H2. The privacy policy at kids.flashget.com/privacy-policy, sections 2.2.3.1 and 2.2.4, read on 23 August 2026, discloses IMEI, IMSI, MAC address, Android ID, operating system version, system language, CPU model, memory and disk usage, and says that third party analytics providers including Google Analytics and Firebase may be used. Whether Google was given an accurate declaration or the card is stale is a question for the operator. This finding states the discrepancy and not its cause.

```
"No data shared with third parties" . "This app may collect these data types: Device
    or other IDs" .
"Data is encrypted in transit" . "You can request that data be deleted"
```

```
"...device information, such as your IMEI, IMSI, MAC, Android ID, operating system
    version, system language, CPU model, memory, hard disk and its usage, etc."
"We may use third-party analytics providers software ... including but not limited to,
     Google Analytics, Firebase."
```

Impact: A parent who relies on the card learns that nothing is shared, while the operator's own policy names Firebase and Google Analytics. The card is the consumer facing summary that Google Play shows before installation, so the discrepancy sits at the point of choice.

Fix: Correct the Data Safety card to list the categories and recipients that the package and the policy show.

H2: The parent app compiles in device identifier probing for the services of seven phone makers

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

The manifest declares the permissions com.asus.msa.SupplementaryDID.ACCESS and freemme.permission.msa and a package query list for the identifier services of Xiaomi, Samsung, Coolpad, OPPO, Huawei, ASUS and Lenovo. The dex files hold the open-source OAID wrapper library com.github.gzuliyujiang.oaid with its implementation classes, the ASUS interface stub and the Huawei open device identifier service stub, and the methods getOaid and isOaidTrackLimited. These services exist to supply an identifier tied to the device and not to the resettable Google advertising ID. The probing sits in the parent app, so it runs on the adult's own phone. The call site was not traced, so whether the lookup runs at every launch or only under conditions, and what is done with the value, are UNVERIFIED. The comparison with AirDroid Parental Control found the same open-source wrapper in that package too, which points to shared ecosystem tooling and not to a shared backend.

```
<uses-permission android:name="com.asus.msa.SupplementaryDID.ACCESS"/>
<uses-permission android:name="freemme.permission.msa"/>
<queries>
    <package android:name="com.mdid.msa"/>
    <package android:name="com.samsung.android.deviceidservice"/>
    <package android:name="com.coolpad.deviceidsupport"/>
    <package android:name="com.heytap.openid"/>          <!-- OPPO -->
    <package android:name="com.huawei.hwid"/>
    <package android:name="com.huawei.hwid.tv"/>
    <package android:name="com.huawei.hms"/>
    <package android:name="com.asus.msa.SupplementaryDID"/>
    <package android:name="com.zui.deviceidservice"/>    <!-- Lenovo, Motorola -->
</queries>
```

```
Lcom/github/gzuliyujiang/oaid/a; ... /i;   Lcom/github/gzuliyujiang/oaid/impl/a; ... /
    e;
Lrepeackage/com/asus/msa/SupplementaryDID/IDidAidlInterface$Stub;
Lrepeackage/com/uodis/opendevice/aidl/OpenDeviceIdentifierService$Stub;
getOaid / getOAID / isOaidTrackLimited
```

Impact: A parental control app that asks several makers' identity services for a persistent identifier collects more than a companion app needs, and an identifier of this kind survives the one control that Android gives the user, the reset of the advertising ID. Google Play restricts such alternate identifiers to specific approved purposes, and a parental analytics purpose is not self-evidently one of them.

Fix: Remove the identifier probing from the parent app, or state its purpose and legal basis and show the call site.

H3: A Tencent Cloud real-time communication, storage and media AI stack carries the camera, audio and screen monitoring, in tension with the policy statement that audio is not stored on servers

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 holds the compiled Tencent packages liteav, trtc, rtmp, live, ugc, cos, qcloud, beacon and mmkv, and a native library of 11.4 MB, libliteavsdk.so in arm64-v8a. The monitoring screens WebRtcActivity, PlayerActivity, ParentCameraSnapShotActivity and ParentScreenRecordActivity run on this stack. The Tencent Cloud Infinite classes in com.tencent.cos.xml.model.ci hold request and response models for face detection, speech recognition, noise reduction, voice synthesis, vocal scoring and live video audit. These are jobs that run on media already held in the cloud storage of the provider. Section 2.2.3.2 of the privacy policy says, for the sound around the child's device, that the operator does not store sound around the device or audio data on any servers. The classes may be unused code or serve another feature, such as moderation of screen snapshots, and the live audio path may use a relay that never stores. That can only be settled by a network capture. Section 9 of the policy says data can be transferred to anywhere in the world and names no mechanism, and no standard clauses, binding corporate rules or adequacy decision are cited.

```
Lcom/tencent/liteav/...   Lcom/tencent/trtc/...   Lcom/tencent/rtmp/...   Lcom/tencent
    /live/...   Lcom/tencent/ugc/...
Lcom/tencent/cos/...      Lcom/tencent/qcloud/...  Lcom/tencent/beacon/...  Lcom/
    tencent/mmkv/...
lib/arm64-v8a/libliteavsdk.so (11.4 MB)
```

```
ci/ai/AIDetectFaceResponse                (face detection)
ci/asr/bean/SpeechJobsDetail              (automatic speech recognition job model)
ci/ai/PostNoiseReductionResponse          (audio noise-reduction job model)
ci/ai/PostVoiceSynthesisResponse          (voice synthesis job model)
ci/ai/VocalScoreResponse                  (vocal scoring job model)
ci/audit/GetLiveVideoAuditResponse        (live-video content-audit job model)
```

```
Privacy policy 2.2.3.2: "We do not store sound around the device or audio data on any
    servers."
Privacy policy 9:      data "can therefore be transferred to anywhere in the world"
```

Impact: The most sensitive capture channel in the product, a child's live camera, audio and screen, is built on a commercial cloud platform run in the PRC, and the policy names no transfer mechanism. Parents and regulators cannot tell from the operator's documents which region processes the data of a child in the Union or whether an impact assessment exists.

Fix: Name the region, the recipient and the Art. 46 mechanism for the monitoring channel, publish the data protection impact assessment, and state whether audio and video touch cloud storage.

H4: The policy names no representative in the Union and no data protection officer, while it defines children of the Union as a processed 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), disclosed as HIGH on 23 August 2026

The privacy policy at kids.flashget.com/privacy-policy, read in full on 23 August 2026, says that a child means a person under 13 for users in the United States and under 16 for users in the Union. It describes geolocation, live audio, notification content and usage statistics of such children in section 2.2.3.2. The only contact in the policy and the Terms of Service is the support mailbox support@flashget.com and a Hong Kong postal address. No representative under Art. 27 and no data protection officer is named. Section 9 is a single paragraph without a transfer mechanism. The Terms of Service designate Hong Kong law and arbitration at the Hong Kong International Arbitration Centre, seated in Hong Kong. The footer of the policy is dated 2023 while the app was last updated in August 2026, and the currency of the policy against the current build was not confirmed. The live policy was not re-read for this report.

```
"Whenever we refer to a child, we mean a child under the age of 13 for US users and a
    child under the age of 16 for EU users."
```

```
Controller:          Hongkong FlashGet Network Technology Co., Ltd.
Address:             FLAT 2304, 23/F HO KING, COMMERCIAL CENTRE, 2-16 FA YUEN STREET,
    MONG KOK KOWLOON, HONG KONG
Contact:             support@flashget.com (the only contact point found)
DPO:                 not found
Art. 27 representative: not found
Terms of Service:    Hong Kong law, arbitration at the HKIAC seated in Hong Kong
```

Impact: A parent in the Union who wants to exercise a right for a child meets a general support mailbox, a Hong Kong address and a Hong Kong arbitration clause. An operator that offers the service to users in the Union and processes children's location and audio has to name a representative under Art. 27, and a large scale systematic monitoring of children is a strong indicator for a data protection officer under Art. 37.

Fix: Name an Art. 27 representative and a data protection officer, give an Union contact for rights requests, and name the transfer mechanism in section 9.

M1: The network security configuration permits cleartext traffic for the whole app, with a private address entry and no certificate pinning

MEDIUM, CVSS v4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), editorial severity HIGH, first stated in this report

The base configuration permits cleartext traffic app-wide. The platform default for target SDK 35 is to forbid it, and the app does not rely on that default. The one scoped entry is the private address 192.168.40.201, consistent with a local testing leftover in a production build. No certificate pin exists anywhere in the file. No cleartext endpoint was identified in the package, so the permission is a capability. The product carries live location, camera and audio streams and notification content of a child. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because the configuration is confirmed in the complete file, the app has more than 10 million installs on Google Play, and the people recorded are children whose location, camera, audio and notification content the app carries.

```
<network-security-config>
    <debug-overrides>
        <trust-anchors><certificates src="user" /></trust-anchors>
    </debug-overrides>
    <base-config cleartextTrafficPermitted="true" />
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">192.168.40.201</domain>
    </domain-config>
</network-security-config>
```

Impact: Any network path that carries a cleartext request of the app lets a party on that path read or alter it. A default that is weaker than the platform default is a weaker starting point for an app that moves the data of a child.

Fix: Set the base configuration to forbid cleartext, remove the private address entry, and consider pinning for the endpoints that carry child media.

Impact Analysis

The people affected are children whose parents or other adults install the child app, and the adults who use the parent app. The policy defines a child as a person under 16 for users in the Union. Further people are those who are near the child's device and appear in camera snapshots or environment captures, such as siblings, classmates, teachers and strangers, and the senders of messages that appear on a mirrored screen or in synchronised notifications.

The weight of the case sits at the concealment function. A product whose parent app contains a function to hide the monitoring app from the monitored person differs from open parental control in the one respect that matters for transparency (C1). The start-up collectors of a paid product (C2), the Data Safety card (H1), the identifier probing (H2), the Tencent stack (H3) and the missing representative (H4) add to it.

What the package shows is labelled capability, policy text and file content. No camera, audio, screen or identifier 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. The Data Safety card says no data is shared and lists device IDs only (H1). The app is paid, and the trial then subscription structure is in the strings (C2).

Step 2, start: at the first process start Firebase, Tencent Beacon and the attribution configuration initialise before any screen, and the package holds no consent platform (C2). The parent app also probes the identifier services of seven phone makers (H2).

Step 3, consent: the parent confirms that they are the guardian or legal agent and that illegal surveillance may be a criminal act. The parent app tells the parent to download the child app from a link in the child's browser (C1).

Step 4, install: the parent can install a disguised version of the child app and hide its icon, and the accessibility step is written for the disguised name (C1).

Step 5, use: camera, audio and screen of the child are monitored through a Tencent Cloud real-time stack, and the policy says audio is not stored on servers (H3). Notifications are synchronised and kept for 48 hours. A permitted cleartext base configuration weakens the default for the traffic (M1).

Step 6, rights: the policy names no representative in the Union and no data protection officer, transfers can go anywhere in the world, and the Terms of Service send disputes to Hong Kong (H4).

Child Protection

The group at the centre of this case is children who are monitored by a parent or another adult through FlashGet Kidsafe. The policy defines a child as under 13 for users in the United States and under 16 for users in the Union. Austria sets the age of digital consent at 14 in § 4 Abs. 4 DSG, and the policy does not mention it. The child does not see the parent app, the Play listing or the policy.

The central point is concealment. A function that installs a disguised version of the child app and hides its icon means that the child cannot recognise that monitoring exists, and cannot ask a trusted person about it. The operator's own consent text acknowledges that unauthorized surveillance may be a criminal act, and places that risk on the parent. The package cannot show who installs the child app and on whose device. The function is therefore available to any adult who can place the app on a phone, not only a parent. Whether the disguised app requests the Android accessibility service was not verified, because the app was not obtained. The strings name that step.

Protections exist and are credited. The policy describes a COPPA flow with an email and a revocation path for children under 13 in the United States. It states that information collected from the accounts of children under 13 is not used for marketing or advertising. allowBackup is set to false in the parent app. The operator's policy shows a 48 hour retention for notification data. No protection is shown for children in the Union that matches the US flow.

Two further points belong here. Camera snapshots and environment captures record whoever is near the child, among them other children who never saw a consent screen. Screen mirroring shows the content of third party apps, such as a friend's message.

Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C2 and H1.

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

Article 5(2), accountability: engaged by C2.

Article 6(1) and Article 7(1): engaged by C2 as a question on the legal basis for the start-up processing.

Article 12 and Article 13: engaged by C1, because the person recorded cannot see the processing, and by H1 for the Data Safety card. Article 13(1)(f) is engaged by H4.

Article 25: engaged by H2.

Article 27: no representative in the Union was found in the policy or the Terms of Service on 23 August 2026 (H4).

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

Article 35: engaged by H3 for the monitoring of children by camera, audio and screen. No assessment was shown.

Article 37: engaged by H4 as an indicator, because large scale systematic monitoring of children is named in the provision.

Articles 44 and 46: engaged by H3, because section 9 of the policy names no transfer mechanism.

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 Data Safety card of the Play listing, captured on 23 August 2026, says no data is shared with third parties and lists only device or other IDs as collected (H1). The listing describes a covert monitoring function only through the parent app's own strings, and whether the Google Play policy on covert monitoring applies was not verified.

Regulatory & Legal Landscape

Hongkong FlashGet Network Technology Co., Ltd., a company in Hong Kong, offers FlashGet Kids 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. Concealed monitoring of a person can also engage national criminal law on surveillance, as the operator's own consent text acknowledges. That law was not assessed in this report.

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 where the source file holds them.

```
Package            com.flashget.parentalcontrol
Version            1.4.1.0 (versionCode 104010008), minSdk 24, targetSdk 35,
    compileSdk 35
XAPK size          94.7 MB
Base APK size      64,107,967 bytes
XAPK SHA-256       c424ab34eec3b2c8c2f973e2f57eebdb3525f7997a3929797561391b042ef5b4
Base APK SHA-256   4b7e2cf8fb73d8143a22f17dd7d871243903e5c2cb5e1f903fc4d2ca13129931
Audit device       none, the app was not installed
Acquisition        APKPure mirror, checked against the Google Play listing, 2026-08-23
```

```
Operator           Hongkong FlashGet Network Technology Co., Ltd.
Address            FLAT 2304, 23/F HO KING, COMMERCIAL CENTRE, 2-16 FA YUEN STREET,
    MONG KOK KOWLOON, HONG KONG
Contact            support@flashget.com
Policy             https://kids.flashget.com/privacy-policy/
Firebase init      com.flashget.parentalcontrol.firebaseinitprovider, initOrder 100,
    directBootAware true
Attribution        res/xml/ga_ad_services_config.xml, allowAllToAccess true
Native library     lib/arm64-v8a/libliteavsdk.so, 11.4 MB
OAID wrapper       com.github.gzuliyujiang.oaid
Cleartext          base-config true, 192.168.40.201
Facebook           facebook_app_id 1234, facebook_client_token 56789 (placeholders)
Maps key           google_maps_key, full value not recorded in the source file
Child app          FlashGet Kidsafe, package name not established
```

```
C1  res/values/strings.xml (Disguise*, HideIcon, Download_Popup_*,
    Installer_Exposure_Warning, Kid_TermsConfirmation_Description)
C2  AndroidManifest.xml, res/xml/ga_ad_services_config.xml, dex strings (Firebase,
    Tencent Beacon, no consent platform)
H1  Play Data Safety card, privacy policy sections 2.2.3.1 and 2.2.4, package contents
H2  AndroidManifest.xml (permissions, queries), dex (com.github.gzuliyujiang.oaid)
H3  libliteavsdk.so, dex (com.tencent.*), privacy policy sections 2.2.3.2 and 9
H4  privacy policy, Terms of Service
M1  res/xml/network_security_config.xml
```

Reproduction: obtain com.flashget.parentalcontrol 1.4.1.0 (104010008), check the SHA-256 values above, decode manifest and resources with apktool without source decode, extract strings from the classes dex files, and read the privacy policy and Terms of Service at the address above. No device, account or network access is needed.

Disclosure Timeline & Outcome

2026-08-23 Notice REF FLASHGETKIDS-2026-R1 at 12:04 UTC to support@flashget.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 16:37 UTC to support@flashget.com. It restated three findings and asked three questions with an answer date of 26 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:04 UTC. It announces 35 days to publication, lists the open points 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 operator publishes a detailed and structured privacy policy that covers data categories, a 48 hour retention window for notification data and a deletion request path. A COPPA flow with a confirmation email and revocation instructions is described for children under 13 in the United States. The policy says that information from the accounts of children under 13 is not used for marketing or advertising. allowBackup is set to false in the parent app, which blocks backup extraction of local data. The Facebook SDK ships with placeholder credentials, so that collector appears inactive in this build. A working Play Billing integration shows a business model of a paid product and not a free front for data collection. The operator states openly that the app needs a child app to be installed on the child’s device.

Residual Risk & Recommendations

Open at the date of publication: all seven findings. The operator has not replied. The child app FlashGet Kidsafe remains the largest open question, because it executes every capture and holds the concealment, and its package name was not established. A network capture would settle the routing of live audio, camera and screen data through Tencent Cloud, and a trace of the call site would settle the identifier probing. A final APK diff against version 1.4.1.0 and a fresh reading of the privacy policy, the Data Safety card and the listing before 21 November 2026 determine the state that the published report records.

Recommendations in order of effect. First, remove the concealment function or tie it to a visible indicator (C1). Second, start Firebase, Tencent Beacon and attribution only after a consent decision (C2). Third, name the region, the recipient and the transfer mechanism for the monitoring channel and publish the impact assessment (H3). Fourth, correct the Data Safety card (H1). Fifth, remove or justify the identifier probing (H2). Sixth, name a representative in the Union and a data protection officer (H4). Seventh, forbid cleartext in the base configuration (M1).

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 FLASHGETKIDS-2026-R1.