# Security & Privacy Disclosure, Final Report

## Nanit for Android (com.nanit.baby)

Written answers received on 29 October and a short message on 16 November, two findings remediated, a medical device certification and a DPIA claimed, open points left unanswered.

**PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 20 NOVEMBER 2026, CORRECTION WINDOW CLOSED 19 NOVEMBER 2026. WRITTEN ANSWERS OF 29 OCTOBER AND 16 NOVEMBER 2026, NO REPLY TO THE OPEN POINTS, NO CORRECTIONS RECEIVED.**

| | |
|---|---|
| **Target** | Udisense, Inc. d/b/a Nanit, New York, USA |
| **Version Audited** | 4.78.0 / 1000453 (2026-08-22) |
| **EU Representative** | MyEDPO Limited, Cork (named in the policy since 2 Nov 2026 check) |
| **Notice / Publication** | 2026-08-22 / 2026-11-20 (90 days) |
| **Findings** | 8: 1 Critical, 2 High, 5 Medium (2 reassessed from High) |
| **Status** | SUBSTANTIVE: 2 remediated (H3, M2), 6 open (C1, H1, H2, H4, M1, M3). Nanit declined further answers on 16 Nov 2026, and no correction arrived by 19 Nov 2026 |
| **SHA-256 (base APK)** | `ff5a76017f830d245389cb81e37f1d5f7321489dbd3ca9d5139d433492dbb297` |

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

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

## Contents


1 Executive Summary 3

2 Finding Status at a Glance 5

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 6

5 Engagement Summary 7

6 Findings 8

6.1 C1: Firebase and the app's own logging pipeline start with the process, before any consent screen, with no functioning consent platform, on an infant audio and video app . . . 8

6.2 H1: Subscription response schema carries ifaType and expectedIfa fields next to live advertising identifier code, disputed by Nanit . . . 10

6.3 H2: Cleartext traffic permitted app-wide and no certificate pinning on a live infant audio and video product . . . 11

6.4 H3: Privacy policy contact block carried an unrendered placeholder and named no EU representative . . . 12

6.5 H4: Privacy policy never treats the infant as a distinct data subject, breathing and sleep data processed with cloud assistance . . . 13

6.6 M1: Google Play Data Safety sharing disclosure is narrower than the privacy policy's own table . . . 14

6.7 M2: Data Safety lists sexual orientation as a collected category, no matching field found in the package . . . 14

6.8 M3: No specific retention period for infant video, audio and breathing data . . . 15

7 Impact Analysis 16

8 The Complete Chain 16

9 Data Protection: Article by Article 17

10 Consumer Protection & Platform Disclosures 18

11 Regulatory & Legal Landscape 18

12 Indicators of Compromise & Reproducible Evidence 19

13 Disclosure Timeline & Outcome 20

14 What Nanit Got Right 21

15 Residual Risk & Recommendations 21

## Executive Summary

Nanit is a camera and sleep coaching app for infants, published on Google Play by Udisense, Inc. of New York under the package com.nanit.baby, rated PEGI 3 with more than 500,000 installs. On 22 August 2026 RFI-IRFOS disclosed eight findings from a root level code analysis of version 4.78.0 under REF NANIT-2026-R1.

The first finding is a pre-consent start. Firebase and the app's own logging pipeline start with the process and the binary holds no working consent platform. Nanit confirmed on 29 October 2026 that Firebase and Mixpanel start with the app and stated that it is removing email addresses and other personal details from the data attached to both (C1). The second sits in the subscription data model, where fields named ifaType and expectedIfa stand next to live advertising identifier code. Nanit says they are unrelated to advertising and that the permissions persist inadvertently. This report holds that finding at MEDIUM until the field contents are shown (H1). Cleartext traffic is permitted for every host of the app, which Nanit explains with captive portals (H2). This report rates H2 at HIGH, because the file permits cleartext for every host of a baby camera product and the explanation does not narrow it.

Two findings are closed. The policy contact block carried the unrendered text [MyEDPO, DPO] and named no EU representative. Nanit corrected it, and RFI-IRFOS verified on 2 November 2026 that the policy now names MyEDPO Limited in Cork (H3). A second finding closed on 16 November 2026: Nanit stated that the Data Safety entry listing sexual orientation was an error in its declaration, and RFI-IRFOS verified on 17 November 2026 that the category no longer appears (M2). On breathing analysis, Nanit states that detection runs on the camera with cloud assistance, that the function is certified as a medical device under Regulation (EU) 2017/745, and that an Article 35 impact assessment exists. The inference in the notice that analysis runs mainly off the device is withdrawn. The statements are recorded as made and the documents are requested (H4). On 16 November 2026 Nanit added that the certification is recorded in EUDAMED and the UK MHRA register and that the assessment is made available to supervisory authorities only. On 17 November 2026 RFI-IRFOS found the manufacturer in the MHRA register (reference 39591, two device entries under GMDN 35194), could not reach the EUDAMED entry because the public search returned HTTP 500 on two attempts, and has seen neither a certificate nor the assessment.

Nanit answered in writing through its Regulatory and Corporate Counsel on 1 October and 29 October 2026. RFI-IRFOS replied on 2 November 2026 with six open points and asked for written answers by 16 November 2026. On 15 November 2026 RFI-IRFOS sent a notice five days before publication. On 16 November 2026 Nanit replied that it does not intend to respond to each further request, pointed to public sources and stated the Data Safety correction. RFI-IRFOS answered on 17 November 2026 with the verification results and accepted factual corrections until 19 November 2026. On the same day the support desk wrote that it had passed the findings to its product and privacy teams. No correction arrived by 19 November 2026, and the only message of 20 November 2026 was an automated satisfaction survey. This report is published after the embargo date of 20 November 2026 was reached.

**Scope:** Root level code analysis of the Google Play release 4.78.0 (versionCode 1000453): manifest, resources, network security configuration, dex string pool across seven classes*.dex files. The privacy policy at nanit.com/policies/privacy-policy and the Google Play listing and Data Safety pages were read from the public sites on 22 August 2026, and the policy was read again on 2 November 2026. No Nanit server, account or database was called, no traffic was intercepted and no runtime instrumentation was used. Statements of Nanit are recorded as made and are marked as not verified where the package cannot show them.

| ID | Severity | Title |
|---|---|---|
| C1 | CRITICAL | Firebase and the app's own logging pipeline start with the process, before any consent screen, with no functioning consent platform, on an infant audio and video app |
| H1 | MEDIUM | Subscription response schema carries ifaType and expectedIfa fields next to live advertising identifier code, disputed by Nanit |
| H2 | HIGH | Cleartext traffic permitted app-wide and no certificate pinning on a live infant audio and video product |
| H3 | HIGH | Privacy policy contact block carried an unrendered placeholder and named no EU representative |
| H4 | MEDIUM | Privacy policy never treats the infant as a distinct data subject, breathing and sleep data processed with cloud assistance |
| M1 | MEDIUM | Google Play Data Safety sharing disclosure is narrower than the privacy policy's own table |
| M2 | MEDIUM | Data Safety lists sexual orientation as a collected category, no matching field found in the package |
| M3 | MEDIUM | No specific retention period for infant video, audio and breathing data |

## Finding Status at a Glance

| ID | Disclosed | This report | Status on 21 November 2026 |
|---|---|---|---|
| C1 | CRITICAL | CRITICAL | Open. Nanit confirmed on 29 Oct 2026 that Firebase and Mixpanel start with the app and is removing email addresses from the attached data. Legal basis and release date asked on 2 Nov 2026. No new statement on 16 Nov 2026, the points stay open. |
| H1 | HIGH | MEDIUM | Disputed by Nanit on 29 Oct 2026. Field contents, SDK component and permission removal asked on 2 Nov 2026. No new statement on 16 Nov 2026. |
| H2 | HIGH | HIGH | Open. Nanit cites captive portals and HTTPS. Hosts, api.nanit.com behaviour, release and pinning asked. No new statement on 16 Nov 2026. |
| H3 | HIGH | HIGH | Remediated. Placeholder gone and EU representative named, verified 2 Nov 2026. |
| H4 | HIGH | MEDIUM | Narrowed. Nanit states camera-side analysis, CE certification and a DPIA. Certificate identifier, Art. 9(2) basis and DPIA asked. On 16 Nov 2026 Nanit stated that the certification is recorded in EUDAMED and MHRA and that the DPIA goes to supervisory authorities only. MHRA registration seen 17 Nov 2026 (no certificate identifier), EUDAMED unreachable (HTTP 500), no certificate and no DPIA seen. |
| M1 | MEDIUM | MEDIUM | Open. Verified on 17 Nov 2026: Data Safety still lists three shared categories, approximate location is listed as collected and not as shared. |
| M2 | MEDIUM | MEDIUM | Remediated. Nanit stated on 16 Nov 2026 that the entry was an error and corrected it. The category no longer appears on the live Play page, verified 17 Nov 2026. |
| M3 | MEDIUM | MEDIUM | Narrowed, open. Plan pages state viewing windows (2 days on Memories, 7 days on Milestones), no deletion period and no period for derived breathing data. Policy of 21 Oct 2026 unchanged in wording. |

## Subject & Operator Analysis

Google Play and the privacy policy name Udisense, Inc., doing business as Nanit, 244 Fifth Avenue, Suite #2702, New York, NY 10011, USA, as the operator. The policy names the United States and Israel as countries where information may be transferred, processed and stored. Contacts in the policy and on Google Play are privacy@nanit.com, help@nanit.com and support@nanit.com. Since the notice, Nanit asks that correspondence goes to privacy@nanit.com with legal@nanit.com in copy. The letters of 1 and 29 October 2026 are signed by Bill Wright, Regulatory and Corporate Counsel.

On 22 August 2026 the policy named no EU representative and showed the placeholder [MyEDPO, DPO]. On 2 November 2026 it names MyEDPO Limited, Cork, as EU representative (H3). No EU main 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.

## Architecture & Data Flow

Nanit is a native Kotlin and Java app with a Kotlin Multiplatform connectivity layer and seven dex files. Live viewing uses WebRTC and a custom RTMP implementation. The four bundled trust anchors are Amazon Root CAs, which shows an AWS backend. Billing runs through Google Play Billing 7.1.1 with no Stripe or RevenueCat. Two-way audio is the documented use of the microphone permission.

At process start, Firebase and the androidx startup providers run, among them the app's own NanitLoggerInitializer. Nanit adds that Mixpanel starts too and records in-app events for access logging, debugging and usage analytics keyed to the account (C1). The subscription model carries ifaType and expectedIfa fields (H1). Nanit states that breathing-motion detection runs on the camera, with cloud-assisted pattern detection and crib confirmation, and that breathing-motion metrics go to the backend and may be kept for the lifetime of the account (H4, M3). Video retention depends on the plan.

No ad mediation SDK was found in the client. No Chinese or sanctioned-jurisdiction SDK and no Tencent, ByteDance, Alibaba, Baidu or Huawei component was found.

## Engagement Summary

The notice REF NANIT-2026-R1 was sent on 22 August 2026 at 12:53 UTC to help@nanit.com, support@nanit.com and privacy@nanit.com, with dsb@dsb.gv.at and edps@edps.europa.eu in copy. The support desk confirmed receipt by automated message the same minute.

On 1 October 2026 Bill Wright acknowledged the notice, apologised for the delay, stated that engineering and data protection teams were reviewing each finding, and asked that correspondence go to privacy@nanit.com with legal@nanit.com in copy. On 29 October 2026 he sent a written response to six points. It confirms Firebase and Mixpanel at start, denies an advertising use of ifaType and expectedIfa, explains the cleartext permission with captive portals, describes camera-side breathing analysis with MDR certification and a DPIA, describes plan-dependent retention, and reports the placeholder corrected.

RFI-IRFOS checked the live policy on 2 November 2026, recorded H3 as settled, and replied the same day to privacy@nanit.com with legal@nanit.com in copy. The reply lists six open points and asks for written answers by 16 November 2026. On 15 November 2026 RFI-IRFOS sent a notice five days before publication to privacy@nanit.com with legal@nanit.com and bill.wright@nanit.com in copy. On 16 November 2026 Bill Wright replied that Nanit has answered in the detail it considers appropriate and does not intend to respond to each further request. He pointed to public sources for retention, the breathing monitoring certification and the Play Data Safety and privacy policy, stated that data protection impact assessments are internal documents made available to supervisory authorities on request, and stated that the Data Safety entry listing sexual orientation was an error that has been corrected. RFI-IRFOS answered on 17 November 2026 to Bill Wright with privacy@nanit.com and legal@nanit.com in copy and recorded the verification results. On 17 November 2026 the support desk also wrote that the findings were submitted to the product and privacy teams for review and cataloguing. No answer to the open points and no factual correction is on record at the date of publication.

## Findings

### C1: Firebase and the app's own logging pipeline start with the process, before any consent screen, with no functioning consent platform, on an infant audio and video app

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9 (CVSS-B), disclosed as CRITICAL on 22 August 2026, initialisation confirmed by Nanit on 29 October 2026, open, rated CRITICAL by blast-radius escalation**

FirebaseInitProvider is directBootAware with initOrder 100, and androidx.startup. InitializationProvider starts NanitLoggerInitializer and WorkManagerInitializer at process start. All seven classes*.dex files contain no OneTrust, Didomi, Usercentrics or other working consent implementation. The IABTCF_CmpSdkID, IABTCF_TCString and IABTCF_PurposeConsents strings exist as inert constants with no class that reads or writes them. No Google Consent Mode flags are set in the manifest. Nanit confirmed in writing on 29 October 2026 that two third-party services start with the app: Firebase for crash reporting, notifications and remote configuration, and Mixpanel for in-app events, access logging, debugging and usage analytics. Nanit states that neither receives video, audio or monitoring data and that neither is used for advertising. Nanit also states that it is removing email addresses and other personal details from the data attached to both. The content of the transmissions was not captured. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the monitored person is an infant who cannot consent, the app sells a paid sleep coaching service, Nanit itself confirms the early start of both services, and no consent mechanism exists in the binary. The CVSS vector scores only the technical exposure of low-sensitivity telemetry.

```
<provider android:authorities="com.nanit.baby.firebaseinitprovider" android:
    directBootAware="true"
          android:exported="false" android:initOrder="100"
          android:name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="com.nanit.baby.androidx-startup" android:exported="
    false"
          android:name="androidx.startup.InitializationProvider">
    <meta-data android:name="com.nanit.baby.init.NanitLoggerInitializer" android:value
    ="androidx.startup"/>
    <meta-data android:name="androidx.work.WorkManagerInitializer" android:value="
    androidx.startup"/>
    <meta-data android:name="androidx.lifecycle.ProcessLifecycleInitializer" android:
    value="androidx.startup"/>
</provider>
<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
```

```
<string name="firebase_database_url">https://nanit-144706.firebaseio.com</string>
<string name="gcm_defaultSenderId">25705829844</string>
<string name="google_api_key">AIzaSyDcp8pEeQBxMMGaiNlNIfS10IaDklF_h5E</string>
<string name="google_app_id">1:25705829844:android:83a90cd56c7431e0</string>
<string name="google_crash_reporting_api_key">AIzaSyDcp8pEeQBxMMGaiNlNIfS10IaDklF_h5E
    </string>
<string name="project_id">nanit-144706</string>
```

The Firebase key is not a secret by Google design. The point of listing it is availability: quota and billing exhaustion against the project, and the question whether the Realtime Database Security Rules deny by default. No call was made against the project. Once shipped, the key cannot be rotated for installed copies.

**Impact:** A parent opening the app to check on a sleeping baby has usage and device signals sent to two analytics and crash services before being asked. Nanit's own letter says it is now removing email addresses and other personal details from the data attached to both services. The household had no choice to make first, and the app belongs to a family's nursery.

**Fix:** Start Firebase Analytics and Mixpanel only after a recorded consent decision, or document why each call is strictly necessary under Article 5(3) of the ePrivacy Directive. Publish the date of the release that removes email addresses from the attached data.

### H1: Subscription response schema carries ifaType and expectedIfa fields next to live advertising identifier code, disputed by Nanit

**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 22 August 2026, disputed by Nanit on 29 October 2026, reassessed to the evidence-only band, open**

The compiled classes SubscriptionStatusResponse and BabySubscription (package nanit.mobile.coreModel.subscription) contain the fields ifaType (type enums.IfaType) and expectedIfa (type ExpectedIfa, a nested object built from String, Integer, String), each with a generated Moshi adapter. The app also contains AdvertisingIdClient code with runtime strings such as AdvertisingIdClient cannot reconnect, and the manifest declares AD_ID, ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION and the Amazon Device Messaging receiver. The privacy policy read on 22 August 2026 states that Nanit shares information for cross-context behavioral advertising and lists sensory data and geolocation data as shared with advertising networks. Disclosed as HIGH on 22 August 2026. On 29 October 2026 Nanit wrote that the fields refer to internal functionality unrelated to advertising identifiers, that the permissions persist inadvertently through SDK components, and that Nanit is taking steps to remove the advertising permission. The package shows the fields and the code. It does not show what expectedIfa holds for an EU subscriber or whether any value reached an advertising network. This report holds the finding at MEDIUM until the two field questions asked on 2 November 2026 are answered.

```
nanit.mobile.coreModel.subscription.SubscriptionStatusResponse
nanit.mobile.coreModel.subscription.BabySubscription
  ifaType      : enums.IfaType
  expectedIfa  : ExpectedIfa(String, Integer, String)
ExpectedIfaJsonAdapter
GeneratedJsonAdapter(ExpectedIfa)
GeneratedJsonAdapter(SubscriptionStatusResponse)
com.google.android.gms.ads.identifier.internal.IAdvertisingIdService
"AdvertisingIdClient cannot reconnect."
"AdvertisingIdClient is not connected."
com.amazon.device.messaging.permission.RECEIVE   (AdmReceiver in manifest)
```

Nanit's privacy policy, read on 22 August 2026, verbatim: We do share information with third parties for the purpose of cross-context behavioral advertising or targeted advertising, and use third-party cookies for such purposes.

**Impact:** If the fields hold what their names suggest, a parent who pays for sleep coaching has an advertising identifier stored with the purchase record of a child's monitoring service. Nanit says they do not, and the package alone cannot settle it. The answer sits with Nanit.

**Fix:** State what IfaType can hold and what expectedIfa contains for an EU subscriber, name the SDK component that requests the permissions, give the release that removes them, and state whether any subscriber record holds an advertising identifier and whether it reached a third party.

### H2: Cleartext traffic permitted app-wide and no certificate pinning on a live infant audio and video product

**MEDIUM, CVSS v4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), editorial severity HIGH, disclosed as HIGH on 22 August 2026, Nanit statement of 29 October 2026 recorded, held at HIGH by blast-radius escalation, open**

The network security configuration is a single base-config with cleartextTrafficPermitted set to true, no domain-config and no pin-set, and the manifest sets usesCleartextTraffic to true. The settings apply to every host the app contacts. The four bundled trust anchors are the Amazon Root CAs 1 to 4, which also show an AWS backend. Live viewing uses WebRTC through NanitWebRtcStreamer and PeerConnectionWrapper plus a custom RTMP implementation. Disclosed as HIGH on 22 August 2026. On 29 October 2026 Nanit wrote that the cleartext permission exists so the camera can connect through captive portals such as hotel networks, that backend traffic uses standard TLS validation, and that communication runs over HTTPS and RTMPS. That statement is taken as made and is not tested here. The configuration permits the opposite and is unchanged in version 4.78.0. CVSS v4.0 scores the configuration at 6.0, which is the MEDIUM band. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because the configuration is confirmed in version 4.78.0 and applies to every host, the product carries live picture and sound from the room of an infant, and the explanation given is a statement that the file itself does not narrow.

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="@raw/aws_ca_1a" />
            <certificates src="@raw/aws_ca_2a" />
            <certificates src="@raw/aws_ca_3a" />
            <certificates src="@raw/aws_ca_4a" />
            <certificates src="system" />
        </trust-anchors>
    </base-config>
</network-security-config>

AndroidManifest.xml  <application android:usesCleartextTraffic="true" ...>
nanit.mobile.core.connect.units.connectivitysuite.baseconnectivity.NanitWebRtcStreamer
PeerConnectionWrapper
multiplatform.rtmp.RTMP
```

**Impact:** The configuration leaves the door open for any connection of the app to fall back to plain HTTP on a hostile network. The product carries a live picture and sound from a baby’s room, so a narrow configuration matters more here than for most apps. Nanit describes a legitimate reason and the fix is a short domain list.

**Fix:** Name the hosts that need cleartext, narrow the configuration to those hosts, state whether api.nanit.com accepts HTTP, and plan certificate pinning for operator-controlled hosts.

### H3: Privacy policy contact block carried an unrendered placeholder and named no EU representative

**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), remediated, verified 2 November 2026, rated HIGH by blast-radius escalation**

On 22 August 2026 the privacy policy dated 10 February 2026 gave this contact block: Nanit [MyEDPO, DPO] 244 Fifth Avenue, Suite #2702 New York, NY 10011 1-866-MYNANIT. No EU postal address and no named representative appeared in the policy or the Play listing, while the policy has a supervisory authority clause for the EEA, Switzerland, the United Kingdom and Brazil. Nanit wrote on 29 October 2026 that the formatting issue is addressed and the policy now has the required contact details. RFI-IRFOS checked the live policy on 2 November 2026: the placeholder is gone and the policy names an EU representative, MyEDPO Limited in Cork. The finding is remediated. 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 no Member State contact was published at disclosure. The score is zero because no technical vector exists.

```
please contact us by email at privacy@nanit.com or at: Nanit [MyEDPO, DPO]244 Fifth
    Avenue,
Suite #2702New York, NY 10011 1-866-MYNANIT
```

**Impact:** Until the correction a parent in the EU who wanted to exercise rights over video and breathing data of their baby found a broken template field and a New York address. Since the correction there is a named representative in Ireland.

**Fix:** Done. Keep the representative and the DPO contact in the policy the app links to.

### H4: Privacy policy never treats the infant as a distinct data subject, breathing and sleep data processed with cloud assistance

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as HIGH on 22 August 2026, narrowed after Nanit statement of 29 October 2026, open**

The only child clause in the policy of 10 February 2026 says the services are not directed to children under 16 as Customers. The same policy lists video and audio of the crib environment, baby name, baby gender, baby date of birth and computer-vision analysis of breathing motion as ordinary usage information. No .tflite, .onnx or .pb model file exists in the package. Disclosed as HIGH on 22 August 2026 with the inference that analysis runs server-side. On 29 October 2026 Nanit wrote that breathing-motion analysis (locating the pattern on the Breathing Wear, tracking it, alerting after 20 seconds without motion) runs on the camera, with cloud-assisted processing for enhanced pattern detection and confirmation that the baby is in the crib. The application itself does not analyse video. Breathing-motion metrics go to the backend for historical insights and may be kept for the lifetime of the account. Nanit states that breathing motion monitoring is certified as a medical device under Regulation (EU) 2017/745 (CE 2797, BSI) and that an Article 35 DPIA exists, prepared with its data protection officer. These are statements of Nanit and are not verified here. The absence of an on-device model in the package does not contradict them, and the inference of the notice that analysis runs mainly off the device is withdrawn. What remains is the policy text that does not address the infant, the derived breathing data kept for the account lifetime, and the open questions on the legal basis. This report holds the finding at MEDIUM.

```
See your baby's breathing motion and get alerts if they need you.
Real-Time Breaths Per Minute - With Breathing Wear, Nanit allows you to see your baby'
    s breathing motion in real time.
Red Alerts If They Need You - Nanit triggers a red alert on your camera and in-app if
    no breathing motion is detected.

Providing the Services to you, including ... using computer vision technologies to
    analyze breathing motion
and baby's behavior such as breathing during sleep and tracking development

The Services are not directed to, nor intended to be operated by, children under 16 (
    or other age as required by
local law), and we do not knowingly collect personal information from children as
    Customers.
```

**Impact:** Breathing and sleep data of a baby are health-adjacent, and they can stay on file for as long as the account exists. A parent reading the policy finds no section written about the infant. Nanit states that a documented impact assessment and a medical device certification exist. Seeing them would settle most of this.

**Fix:** Provide the CE certificate identifier and notified body, the Article 9(2) basis for derived breathing and sleep data, and the Article 35 DPIA or a summary. Add an infant-specific section to the policy.

### M1: Google Play Data Safety sharing disclosure is narrower than the privacy policy's own table

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), open, verified on 17 November 2026**

The Data Safety entry reads: This app may share these data types with third parties: Personal info, App activity, and App info and performance. The CCPA table in the privacy policy lists geolocation data (approximate location) shared with service providers, advertising networks, data analytics providers and government entities, and sensory data (audio, electronic, visual, thermal, or similar information) shared with service providers. Both are from Nanit and both were live on 22 August 2026. Nanit wrote on 29 October 2026 that it is reviewing the discrepancies and will update where necessary. This is a transparency finding with no technical vector. On 17 November 2026 the live Data Safety entry still named the same three shared categories. Approximate location is listed as collected and not as shared, while the policy table updated on 21 October 2026 lists geolocation data with advertising networks among the recipients.

**Impact:** A parent choosing a baby monitor reads the store label first. If the label shows less sharing than the policy, the parent decides on a smaller picture than the controller itself describes.

**Fix:** Align the Data Safety entry and the policy, and give the date of the correction.

### M2: Data Safety lists sexual orientation as a collected category, no matching field found in the package

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), remediated, verified on 17 November 2026**

The Data Safety detail for Personal info on 22 August 2026 listed: Name, Email address, User IDs, Address, Phone number, Sexual orientation, and Other info. A search of res/values/strings.xml and all seven classes*.dex files found no onboarding field, profile field or survey string for sexual orientation. The orientation strings in the package (orientation_left, orientation_right, title_settings_orientation) concern crib and device placement. Either a collection point exists outside the mobile client or the form is inaccurate. This is a transparency finding with no technical vector. Nanit wrote on 16 November 2026 that the entry listing sexual orientation was an error in its declaration and has been corrected. The live Play page read on 17 November 2026 no longer shows the category. Personal info lists Name, Email address, User IDs, Address, Phone number and Other info.

**Impact:** A category of data as sensitive as sexual orientation, listed without explanation on a baby monitor, leaves a parent unable to tell what the company holds.

**Fix:** Corrected by Nanit before 16 November 2026. The date of the correction was not given.

### M3: No specific retention period for infant video, audio and breathing data

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), narrowed, open, no deletion periods in days given**

The Retention of Personal Information section in the policy read on 22 August 2026 gives no period for any category. The app has a paywalled Days of Video History feature, so a numeric window exists in operation. Nanit wrote on 29 October 2026 that video retention depends on the subscription plan, that derived breathing, motion and sleep information may be retained for the lifetime of the account, and that on account deletion video and derived data are permanently anonymised. No periods in days were given. This is a transparency finding with no technical vector. On 16 November 2026 Nanit pointed to its membership pages and support center. They state viewing windows per plan, for example 2 days of continuous video history on Memories and 7 days on Milestones, read on 17 November 2026. A viewing window does not state when footage is deleted. No period is given for derived breathing and sleep data, which Nanit said on 29 October 2026 may be kept for the lifetime of the account. The privacy policy of 21 October 2026 keeps the general wording.

```
We store the personal information we collect as described in this Privacy Policy for
    as long as you use
our Services or as necessary to fulfill the purpose(s) for which it was collected,
    provide our Services,
resolve disputes, establish legal defenses, conduct audits, pursue legitimate business
     purposes, enforce our
agreements, and comply with applicable laws.
```

**Impact:** A parent cannot tell how long footage of their baby’s room and months of breathing data stay on file, or what changes when they stop paying.

**Fix:** State the retention in days for each plan, for saved clips, continuous history and derived breathing data.

## Impact Analysis

The people affected are households with a Nanit camera and, behind them, infants who are monitored around the clock and cannot consent. The service is paid, with a sleep coaching subscription, and the company sells hardware, so the arguments that tracking funds a free service do not apply. Nanit itself says a Nanit login is the front door to a family's nursery, and that parents ask for account access records more often than users of a typical service.

C1 affects every launch for every user, and Nanit confirms the early start of Firebase and Mixpanel and the removal of email addresses and other personal details from the attached data. H2 concerns the paths that carry a live picture of a baby's room. H1 and H4 concern whether an advertising identifier sits with a purchase record and how breathing and sleep data are handled, and in both cases Nanit has given a written account that this report records as made. The remaining Medium items are disclosure gaps: store labels, a sexual orientation entry and missing retention periods.

The harm demonstrated in the package is a harm of design and transparency. No access to video, audio, accounts or databases was shown, and none was tried.

## The Complete Chain

Step 1, purchase and install: a household buys a Nanit camera and installs the app. A subscription for sleep coaching is offered through Google Play Billing (H1).

Step 2, first launch: Firebase, the logging initializer and, according to Nanit, Mixpanel start with the process, before the login screen and before any consent screen (C1). Cleartext traffic is permitted for every host (H2).

Step 3, account and baby profile: the policy lists baby name, gender, date of birth and video and audio of the crib environment as usage information. The only child clause addresses adult customers (H4).

Step 4, operation: detection of breathing motion runs on the camera, with cloud assistance, and metrics reach the backend and can stay for the account lifetime (H4, M3). Live view uses WebRTC and RTMP.

Step 5, the parent tries to act: before the correction the policy gave a placeholder and a New York address (H3). The Play label and the policy describe different sharing (M1, M2), and no retention period is stated (M3).

## Data Protection: Article by Article

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1 and M1. M2 was engaged and is remediated.

Article 5(1)(b) and (c), purpose limitation and minimisation: engaged by H1, as a question about the ifaType and expectedIfa fields.

Article 5(1)(e), storage limitation: engaged by M3.

Article 5(2), accountability: engaged by C1 and H4. Nanit states that a DPIA exists and has been asked to provide it.

Article 6(1) and Article 7(1): engaged by C1. Nanit relies on legitimate interest in account security for Mixpanel records. The question of the basis for Firebase Analytics before any consent is open.

Article 4(5), pseudonymisation: Nanit says it is reducing the attached data to an internal identifier. Pseudonymised data remains personal data.

Article 8, child's consent: engaged by H4, because the infant cannot consent and the account holder is the adult customer.

Article 9(2), special categories: engaged by H4. The legal basis for derived breathing and sleep data is asked.

Article 12(1) and Article 13(1)(a) and (b), (c) and (e), and 13(2)(a): H3 and M2 were engaged and are remediated. M1 and M3 remain engaged.

Article 25, data protection by design and by default: engaged by C1 and H1.

Article 27(1), representative: engaged by H3, met by the representative named since the correction.

Article 32(1)(a) and (b): engaged by H2 and by the Firebase project exposure in C1.

Article 35, impact assessment: asserted by Nanit, requested by RFI-IRFOS. Nanit stated on 16 November 2026 that it is made available to supervisory authorities on request and not to third parties.

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

## Consumer Protection & Platform Disclosures

The Google Play listing rates the app PEGI 3. The Data Safety page on 22 August 2026 said the app may share personal info, app activity, and app info and performance with third parties, and listed sexual orientation among collected personal info (M1, M2). The privacy policy lists wider sharing in its California table. Nanit wrote on 29 October 2026 that it reviews its Data Safety disclosures and will update where necessary. The live label was read again on 17 November 2026. The sexual orientation category no longer appears (M2, remediated). The three shared categories are unchanged and approximate location is listed as collected and not as shared (M1).

## 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. The operator is established in the United States and offers its product to EU households, which brings Article 3(2) GDPR into play.

Nanit states that breathing motion monitoring is certified as a medical device under Regulation (EU) 2017/745 with the number CE 2797 and the notified body BSI, and under the UK Medical Devices Regulations 2002. RFI-IRFOS asked on 2 November 2026 for the certificate identifier, because 2797 reads as a notified-body number. The statement is recorded as made. This report does not assess the certification. 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. 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. All values are given in full.

```
Package            com.nanit.baby
Version            4.78.0 (versionCode 1000453), analysed 2026-08-22
base.apk SHA-256   ff5a76017f830d245389cb81e37f1d5f7321489dbd3ca9d5139d433492dbb297
XAPK SHA-256       85ffcd3fb0d2ecacea066a0829fa0c2b84401d2739ef70fdf7eb66ceb9413b1c

Firebase project   nanit-144706
google_api_key     AIzaSyDcp8pEeQBxMMGaiNlNIfS10IaDklF_h5E
google_app_id      1:25705829844:android:83a90cd56c7431e0
gcm_defaultSenderId 25705829844
Database URL       https://nanit-144706.firebaseio.com
Backend hosts named in the notice   api.nanit.com, app.nanit.com
```

```
C1  AndroidManifest.xml: FirebaseInitProvider, androidx.startup.InitializationProvider
     (NanitLoggerInitializer), AppMeasurement*
C1  7 classes*.dex files: no working consent implementation, inert IABTCF_* constants
H1  classes*.dex: nanit.mobile.coreModel.subscription.SubscriptionStatusResponse,
    BabySubscription, ExpectedIfaJsonAdapter, AdvertisingIdClient
H2  res/xml/network_security_config.xml and usesCleartextTraffic in AndroidManifest.
    xml
H3  https://www.nanit.com/policies/privacy-policy, contact section (10 February 2026
    version and 2 November 2026 check)
H4  res/values/strings.xml breathing strings, policy sections Children's Information
    and How We Use Your Information
M1  play.google.com/store/apps/datasafety?id=com.nanit.baby against the California
    table of the policy
M2  Data Safety detail for Personal info
M3  policy section Retention of Personal Information
```

Reproduction: obtain com.nanit.baby 4.78.0 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 NANIT-2026-R1 to help@nanit.com, support@nanit.com and privacy@nanit.com, CC DSB and EDPS. Automated receipt from the support desk the same minute.

2026-10-01 Bill Wright, Regulatory and Corporate Counsel, acknowledges the notice, apologises for the delay and asks that correspondence go to privacy@nanit.com with legal@nanit.com in copy.

2026-10-29 Written response from Nanit on six points: Firebase and Mixpanel at start, ifaType and expectedIfa unrelated to advertising, cleartext for captive portals, camera-side breathing analysis with MDR certification and a DPIA, plan-dependent retention, DPO contact details corrected.

2026-11-02 RFI-IRFOS verifies the live policy, records H3 as settled, and sends six open points to privacy@nanit.com with legal@nanit.com in copy. Written answers requested by 16 November 2026.

2026-11-15 RFI-IRFOS sends a notice five days before publication to privacy@nanit.com with legal@nanit.com and bill.wright@nanit.com in copy, listing the status of all eight findings and the six open points.

2026-11-16 Bill Wright replies that Nanit does not intend to respond to each further request, points to public sources, states that data protection impact assessments are made available to supervisory authorities on request and that the Data Safety entry listing sexual orientation was an error that has been corrected.

2026-11-17 RFI-IRFOS verifies the sources: M2 remediated, M1 open, M3 narrowed, MHRA registration found (reference 39591), EUDAMED unreachable (HTTP 500 on two attempts). Answer sent to Bill Wright with privacy@nanit.com and legal@nanit.com in copy. Factual corrections accepted until 19 November 2026.

2026-11-17 The Nanit support desk (help@nanit.com, signed Mackenzie T) writes that the findings and requests were submitted to the product and privacy teams for review and cataloguing, and invites factual corrections before 19 November 2026. Whether a person or a template wrote the message is not verified.

2026-11-19 Correction window closes. No factual correction from Nanit is on record.

2026-11-20 Automated satisfaction survey from the support desk (Nanit Family Support), no content on the findings.

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

## What Nanit Got Right

Nanit answered in writing through named counsel, with specific content on every one of the six points, and it corrected the policy contact block and named an EU representative by the time of the check of 2 November 2026. It stated that it is removing email addresses from the data attached to Firebase and Mixpanel and that it is removing the unnecessary advertising permission. It also corrected the Data Safety entry on sexual orientation and named the entry as its own error in writing on 16 November 2026. The package has allowBackup set to false, real two-factor authentication (TwoStepVerificationSetupActivity, MfaEnforceActivity), a microphone permission tied to the documented two-way audio feature, no ad mediation SDK, no Chinese or sanctioned-jurisdiction SDK, and billing only through Google Play Billing 7.1.1.

## Residual Risk & Recommendations

Open at the date of publication: C1, H1, H2, H4, M1 and M3, with M3 narrowed. Remediated: H3 and M2. Written answers were requested by 16 November 2026 and Nanit declined further answers on that date, and no factual correction arrived before the correction window closed on 19 November 2026.

What the package cannot settle and Nanit can: the legal basis and release date for the pre-consent start (C1), the contents of ifaType and expectedIfa for EU accounts and whether the advertising identifier was ever stored or shared (H1), the host list for cleartext and the behaviour of api.nanit.com (H2), the CE certificate identifier, the Article 9(2) basis and the DPIA (H4), the correction date for the store label (M1), and retention in days per plan (M3).

Recommendations: gate Firebase Analytics and Mixpanel behind a recorded consent decision or document strict necessity, remove the advertising permissions, narrow cleartext to named hosts and add pinning for operator-controlled hosts, add an infant-specific section to the policy, publish retention periods per plan, and align the Play Data Safety entry with the policy.

This report is published after the embargo date. Statements are limited to the package and to the public documents and written letters named above.

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