Security & Privacy Disclosure, Final Report

eufy Clean for Android (com.eufylife.smarthome)

A vacuum that recognizes people as an obstacle category and lets the account holder donate the photo, and the fixes Anker reported as completed on 18 November 2026.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. THREE SUBSTANTIVE REPLIES, THE LATEST ON 18 NOVEMBER 2026 WITH A REMEDIATION UPDATE THAT RFI-IRFOS HAS NOT VERIFIED.

Target	Anker Innovations group, joint controllers named in the privacy notice: Fantasia Trading LLC (Ontario, California), Anker Innovations Deutschland GmbH (Düsseldorf), Anker Innovations (Netherlands) B.V. (Rotterdam), Anker Innovations Limited (Hong Kong)
Versions Audited	3.19.0 / versionCode 1040 (analysed 2026-08-23), 137.9 MB, internal namespace com.oceanwing.eufyhome
Supervisory Authority	Datenschutzbehörde, Austria, informed for transparency. No lead authority is assumed, the privacy notice lists several joint controllers.
Notice / Publication	2026-08-23 / 2026-11-21 (90 days)
Findings	10: 1 High, 1 Medium, 8 Low (six from the first notice, re-assessed, and four added)
Status	THREE SUBSTANTIVE REPLIES (26 AUGUST, 8 SEPTEMBER AND 18 NOVEMBER 2026). THE REPLY OF 18 NOVEMBER ANSWERS THE THREE OUTSTANDING QUESTIONS AND REPORTS TWO REMEDIATION ITEMS AS COMPLETED AND THE IN-APP DISCLOSURE AS SCHEDULED FOR THE END OF NOVEMBER 2026. These statements are stated by the operator, not verified by RFI-IRFOS.
SHA-256 (base APK)	`db716d3e9402e5fb87fad40a57230489e29decf8e83eafa4d258b942e0449515`

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

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

Contents

1 Executive Summary 4

2 Finding Status at a Glance 6

3 Subject & Operator Analysis 7

4 Architecture & Data Flow 7

5 Findings 8

5.1 C1: People as an obstacle category, a photo donation flow chosen by the account holder, and cloud-persisted, shareable room maps . . . 8

5.2 C2: Hardcoded Tuya ThingSmart and MobTech credential pairs and a Firebase key . . . 10

5.3 C3: Camera-backend (VSAAS) configuration with a mainland-China endpoint and a Shenzhen storage bucket inside a cleaning app . . . 12

5.4 H1: MobTech ShareSDK and its consent string for collecting the installed-app list 14

5.5 H2: Network security configuration permits cleartext traffic for every domain and sets no pinning . . . 15

5.6 H3: No consent-management platform found, full Firebase suite present, Crashlytics collection enabled . . . 16

5.7 H4: Self-declared transfers to China and China-headquartered group processors, unnamed . . . 17

5.8 M1: Play Data Safety label omits location, photos and audio although the permissions are requested . . . 18

5.9 M2: Exported login activity and exported BLE companion service . . . 18

5.10 M3: android:persistent set to true at application level . . . 19

6 Impact Analysis 19

7 The Complete Chain 20

8 People in the Photo & Bystanders 20

9 Data Protection: Article by Article 21

10 Regulatory & Legal Landscape 22

11 Indicators of Compromise & Reproducible Evidence 22

12 Disclosure Timeline & Outcome 23

13 What Anker Got Right 24

14 Residual Risk & Recommendations 25

Executive Summary

eufy Clean is the control app for eufy robot vacuums, lawn mowers and other cleaning hardware, published on Google Play by Anker with more than one million downloads. On 23 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF EUFYCLEAN-2026-R1 after a root level code analysis of version 3.19.0. The notice itemised six findings, three Critical and three High, and asked three written questions.

The case turns on one feature. The app ships a labelled obstacle-recognition list of 23 categories that includes People, a Real Obstacle Photos function, and a flow named donation. The string reads: By donating to this event, you agree to share this capture and device log with eufy and give us permission to use it for further analysis and algorithm improvement. The account holder taps donate. The person in the photo, a child, a partner, a visitor or a cleaner, never sees the screen. Room maps are modelled with a cloud map ID and can be shared with a second account. Anker's privacy notice of about 122,000 characters discloses camera-based navigation in general terms and contains no occurrence of donat.

Around that feature sit the other findings. Two IoT credential pairs, Tuya ThingSmart and MobTech ShareSDK, and a Firebase key are readable in the package. A configuration for the eufy security camera backend (VSAAS) with a mainland-China QA endpoint and an Alibaba Cloud bucket in Shenzhen is hardcoded in a cleaning app. A MobTech consent string describes collection of the installed-app list. Cleartext traffic is permitted for every domain. The privacy notice admits processing by China-headquartered group entities.

This report is stricter than the first notice. The six findings of the notice are all reassessed. One Critical label becomes High, one becomes Medium and one becomes Low. All three High labels become Low. Four further findings from the same analysis, H3, M1, M2 and M3, were not itemised in the notice and are added, all at Low. The reasons are given in each finding.

Anker answered substantively three times, which sets this case apart from the other two in this wave. On 26 August 2026 (ticket ANKER-TNC1054839961) it described on-device de-identification of people before upload, called the credentials standard SDK integration artifacts, called the VSAAS code dormant legacy, confirmed the cleartext finding and said it would restrict cleartext and add pinning. On 8 September 2026 it committed to an enhanced in-app disclosure and to removal of the VSAAS code, both by the end of October 2026, and declined to rotate any of the credentials. RFI-IRFOS asked three questions on 8 September 2026 with a deadline of 22 September 2026. Anker acknowledged them on 9 September 2026. RFI-IRFOS sent a notice on 15 November 2026 stating publication for 21 November 2026. On 18 November 2026 Anker answered the three questions: it states that a DPIA under Art. 35 was conducted for the People recognition and donation processing, that faces and human forms are irreversibly masked on the device, and that it reviewed the Firebase project eufy-prod-158108 and found no public read or write access risks. It reports the VSAAS code-path removal and the Firebase key restrictions as completed, and the enhanced in-app disclosure as scheduled for the end of November 2026, a month after the date it gave on 8 September. These statements are stated by the operator, not verified by RFI-IRFOS. The report is published on 21 November 2026, 90 days after delivery.

Scope: Root level code analysis of eufy Clean 3.19.0 (versionCode 1040): AndroidManifest.xml, decoded resources, 15 classes dex files with about 6,087 unique class-descriptor strings and the dex string pool. No full smali pass was run, so every claim that would need code flow beyond strings and manifest is marked UNVERIFIED. The package came from the APKPure mirror after its version code matched the live Google Play listing exactly and its size matched the archived file at 144,648,007 bytes, because the audit device was not reachable on the analysis day. Anker's privacy notice (www.eufy.com/pages/privacy-policy, Anker Group notice of about 122,000 characters) and the Google Play listing were read on 23 August 2026. No account was created, no Anker server was called, no key was tested and no runtime instrumentation was used. Statements by Anker about on-device processing, server-side flags and the state of remediation are vendor statements and are UNVERIFIED. Builds after 3.19.0 were not analysed for this report. CVSS v4.0 measures exploitability. Most findings here concern data governance, so CVSS-B scores are low and the report states where the rating is raised for the people affected.

ID	Severity	Title
C1	HIGH	People as an obstacle category, a photo donation flow chosen by the account holder, and cloud-persisted, shareable room maps
C2	MEDIUM	Hardcoded Tuya ThingSmart and MobTech credential pairs and a Firebase key
C3	LOW	Camera-backend (VSAAS) configuration with a mainland-China endpoint and a Shenzhen storage bucket inside a cleaning app
H1	LOW	MobTech ShareSDK and its consent string for collecting the installed-app list
H2	LOW	Network security configuration permits cleartext traffic for every domain and sets no pinning
H3	LOW	No consent-management platform found, full Firebase suite present, Crashlytics collection enabled
H4	LOW	Self-declared transfers to China and China-headquartered group processors, unnamed
M1	LOW	Play Data Safety label omits location, photos and audio although the permissions are requested
M2	LOW	Exported login activity and exported BLE companion service
M3	LOW	android:persistent set to true at application level

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	HIGH	Notice finding 1. Anker states on 18 November 2026 that a DPIA exists and that masking is irreversible on the device; the enhanced in-app disclosure moved from the end of October to the end of November 2026. Not verified. Reassessed.
C2	CRITICAL	MEDIUM	Notice finding 2. Anker declines rotation for all three credentials. On 18 November 2026 it states that the Firebase project was reviewed and both Firebase API keys are now bound to the package name and signing certificate. Not verified. Reassessed.
C3	CRITICAL	LOW	Notice finding 3. Anker states on 18 November 2026 that the VSAAS code-path removal is completed. Not verified against a current build. Reassessed.
H1	HIGH	LOW	Notice finding 4. Anker: collection disabled server-side, removal in next update. Reassessed.
H2	HIGH	LOW	Notice finding 5. Anker confirmed on 26 August 2026, restriction and pinning announced. No completion reported in the reply of 18 November 2026. Reassessed.
H3	Not itemised	LOW	Added in this report.
H4	HIGH	LOW	Notice finding 6. Anker names SCCs with TIA. Entity naming not confirmed. Reassessed.
M1	Not itemised	LOW	Added in this report.
M2	Not itemised	LOW	Added in this report.
M3	Not itemised	LOW	Added in this report.

Subject & Operator Analysis

eufy Clean (package com.eufylife.smarthome, internal namespace com.oceanwing.eufyhome, launch activity WelcomeActivity) is listed on Google Play as eufy Clean(EufyHome) by Anker with more than one million downloads and PEGI 3. It is the control app for eufy robot vacuums, lawn mowers and other cleaning hardware.

Anker's privacy notice names joint controllers: Fantasia Trading LLC, 5350 Ontario Mills Pkwy, Suite 100, Ontario, CA 91764, USA. Anker Innovations Deutschland GmbH, Prinzenallee 15, 40549 Düsseldorf. Anker Innovations (Netherlands) B.V., Wilhelminakade 1, 103, 3072AP Rotterdam. Anker Innovations Limited, Unit 56, 8th Floor, Tower 2, Admiralty Centre, 18 Harcourt Road, Hong Kong, the fallback controller where no local entity exists. China-headquartered intra-group processors are named by function only. The contacts used were DPO@anker.com and support@eufylife.com, and the replies came from dpo@anker.com under ticket ANKER-TNC1054839961.

The package targets Android API 35 with minSdkVersion 24 and ships 15 classes dex files with 336 declared activities, consistent with a multi-brand platform app.

Architecture & Data Flow

- App to robot through the Tuya ThingSmart IoT platform (com.thingclips.smart.*), which authenticates and routes device-control traffic.
- Obstacle recognition on the robot with a 23-category taxonomy plus a People category. Whether inference runs on the device or on a server is UNVERIFIED. Anker states that de-identification happens on the device before transmission.
- Real Obstacle Photos: the app shows real photos of detected obstacles. A donation flow lets the account holder send a capture and a device log to eufy.
- Map: room names, floor types and a cloud map ID, shareable through the device-sharing actions.
- Region-partitioned endpoint families with China-region literals (aiot-clean-api-cn.anker.com.cn, cn-eufy.oss-cn-shenzhen.aliyuncs.com) and a runtime domain-placeholder table for several brands.
- Third-party SDKs: Firebase (Crashlytics enabled), MobTech ShareSDK and the Google Advertising ID client.

The architecture is a shared multi-brand platform. The risks sit in what is photographed and who decides, what is kept in the cloud and who can see it, and which entities in which countries handle it.

Findings

C1: People as an obstacle category, a photo donation flow chosen by the account holder, and cloud-persisted, shareable room maps

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), reassessed from CRITICAL in the first notice, rated HIGH by blast-radius escalation

res/values/strings.xml holds 24 ai_recognize_ strings, among them ai_recognize_people (People), ai_recognize_pets, ai_recognize_poop and ai_recognize_cat_litter_box, plus the donation string ai_recognize_donating and the Real Obstacle Photos strings. The dex holds MapRoomName, getAllRoomFloorType, setCloudMapid and clearCloudMapid and the device-sharing actions CleanInviteShareDeviceAction and CleanAcceptShare-DeviceAction. Anker's privacy notice has no occurrence of donat.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to HIGH because CVSS gives a feature with no demonstrated exposure 0.0. The finding is rated HIGH because the category list names people, because the person who may be photographed is a bystander such as a child, a partner, a visitor or a cleaner and not the account holder who taps donate, and because the room map is held under a cloud map ID that a second account can be given. CRITICAL, as disclosed on 23 August 2026, is withdrawn because the payload, the retention and the point at which processing happens were not observed, and because Anker states that people are irreversibly de-identified on the device before anything is transmitted. That statement is UNVERIFIED.

```
ai_recognize_bed Bed
ai_recognize_chair Chair
ai_recognize_curtains Curtains
ai_recognize_mirror Mirror
ai_recognize_sofa Sofa
ai_recognize_table Table
ai_recognize_wardrobe Cabinet
ai_recognize_flower_pot Flower Pot
ai_recognize_power_strip Power Strip
ai_recognize_refrigerator Refrigerator
ai_recognize_scale Scale
ai_recognize_sports_shoes Shoes
ai_recognize_toys_puzzles Toys/Puzzles
ai_recognize_electric_fan Electric Fan
ai_recognize_electrical_wires Electrical Wires
ai_recognize_fabric_clothing Fabric/Clothing
ai_recognize_liquid_stains Liquid Stains
ai_recognize_tissues Tissues
ai_recognize_cat_litter_box Cat Litter Box
ai_recognize_pet_bed Pet Bed
ai_recognize_pet_bowls Pet Bowls
ai_recognize_pets Pets
ai_recognize_poop Poop
ai_recognize_people People
```

```
<string name="ai_recognize_donating">By donating to this event, you agree to share
    this capture and
device log with eufy and give us permission to use it for further analysis and
    algorithm
improvement.</string>
<string name="ai_recognize_turnon_pohoto">Click to enable Real Obstacle Photos</string
    >
<string name="ai_recognize_nextcleaning">Next obstacle detection will display real
    photos</string>
```

```
com/anker/clean_sdk/clean_map/map_bean/MapRoomName
com/anker/clean_rn_bridge/view/EHMapView$getAllRoomFloorType$1
com/anker/esiotkit/clean_device/domain/thing/actions/CleanAcceptShareDeviceAction
com/anker/esiotkit/clean_device/domain/thing/actions/CleanInviteShareDeviceAction
com/anker/esiotkit/clean_device/domain/thing/actions/CleanShareDeviceAction
com/anker/eufy/ota/view/ShareDeviceOTAActivity
setCloudMapid / clearCloudMapid / setMapId / setRoomName
com/acc/map/ui/pin/RoomNamePinView
```

What the evidence shows: a taxonomy of 23 obstacle categories plus an extra category for people, a function that captures real photos of what triggered a detection, and a separately named flow through which the account holder sends a capture and a device log to eufy for algorithm improvement. The map is modelled with a cloud map ID, so the floorplan is stored under an identifier the client can set and clear. A sharing subsystem gives a second account access to a device. What it does not show: a live payload, whether people detections trigger the donation prompt more often than furniture, whether photos are kept after training, where recognition runs, and whether the screen distinguishes a photo of a person from a photo of furniture before the consent tap. The strings carry one consent sentence for all categories.

Policy and code: Anker's privacy notice, read on 23 August 2026, does disclose generally that robot vacuums with cameras may capture images or video for navigation and obstacle avoidance if consent was obtained, and that information about the home environment such as floorplans, types of flooring and the existence and types of objects is collected. That is a better starting disclosure than the one found for the other robot vacuum in this wave. What it does not name is a People category, the donation mechanism and the fact that the person captured is often not the account holder. The finding is narrower than a claim of no disclosure.

Anker's reply of 26 August 2026 states that the account holder's consent activates the feature (Art. 6(1)(a)), that the device applies on-device, irreversible de-identification such as pixel-level blurring or masking to every detected human form before any transmission, that the purpose is training the obstacle model and not identifying anyone, and that no separate legal basis for bystanders is therefore needed. Its reply of 8 September 2026 states that the People classification is a downstream labelling step on already de-identified data, that ISO 27001, ISO 27701 and EN 303 645 inform its practice, and that it will enhance the in-app Experience Improvement Program screen to say so by the end of October 2026, without amending the privacy policy. Its reply of 18 November 2026 states: "Yes. We have conducted a Data Protection Impact Assessment (DPIA) under Article 35 of the GDPR" for the People recognition and donation processing. It adds that donated faces and human forms are irreversibly masked on the device and that Anker therefore does not treat the donated data as personal data, that the account holder's decision authorises only the account holder's own donation, and that the enhanced disclosure is now expected by the end of November

2026. All of these are vendor statements and are stated by the operator, not verified by RFI-IRFOS. The DPIA itself was not provided, and no test or audit showing that masking precedes classification was supplied. If the statements are accurate, the processing of bystanders is considerably narrower than the strings suggest. The three standards named on 8 September are certifications of management systems and are not a DPIA.

Impact: A household with an eufy robot owns a camera that is built to recognize people on the floor, and the person who decides whether a photo goes to the manufacturer is the account holder. The person in the photo can be a child at play, a partner asleep or an elderly relative. They did not choose it and cannot see the screen. A family member with share access can be given the room map of the home.

Fix: Name the People category and the donation flow in the privacy policy as a distinct processing activity, publish the DPIA conclusion, show the audit that establishes that de-identification precedes classification, and state how information reaches the person in the photo.

C2: Hardcoded Tuya ThingSmart and MobTech credential pairs and a Firebase key

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

AndroidManifest.xml carries THING_SMART_APPKEY and THING_SMART_SECRET for the Tuya ThingSmart IoT platform and Mob-AppKey and Mob-AppSecret for MobTech ShareSDK. res/values/strings.xml carries a Firebase API key (also declared as crash-reporting key), app ID, database URL, storage bucket, project ID and web client ID. All values are extractable with apktool from any Play Store download. The functional scope of the secrets is UNVERIFIED.

```
<!-- AndroidManifest.xml -->
<meta-data android:name="THING_SMART_APPKEY" android:value="fdkdn5hpmujkvpfgv3pc"/>
<meta-data android:name="THING_SMART_SECRET" android:value="3
    w38pdhqyqtrcv3y898ytqwt85katjgg"/>
<meta-data android:name="Mob-AppKey" android:value="3504ca74a0820"/>
<meta-data android:name="Mob-AppSecret" android:value="77797
    af3d4cbfab0d474e53a914e5312"/>

<!-- res/values/strings.xml -->
<string name="google_api_key">AIzaSyDTSD_9xTfo3bTuOCmEatTp-lGbFmm7wsA</string>
<string name="google_crash_reporting_api_key">AIzaSyDTSD_9xTfo3bTuOCmEatTp-lGbFmm7wsA
    </string>
<string name="google_app_id">1:466383759367:android:f4f9c96472b0e050</string>
<string name="firebase_database_url">https://eufy-prod-158108.firebaseio.com</string>
<string name="google_storage_bucket">eufy-prod-158108.appspot.com</string>
<string name="project_id">eufy-prod-158108</string>
<string name="default_web_client_id">466383759367-3c35hr3r2bb1433ijr5a84v3ch8scpc1.
    apps.googleusercontent.com</string>
```

The Tuya ThingSmart pair is the platform-level authentication secret of the white-label IoT cloud SDK (com.thingclips.smart.*, present throughout the dex) that routes this app's device-control traffic. The second pair authenticates MobTech ShareSDK. No credential was used against any server. Anker's reply of 26 August 2026 describes them as standard integration

artifacts mandated by the vendors' guides and says it would explore dynamic provisioning or backend proxying. Its reply of 8 September 2026 states that the review is complete, that the MobTech key cannot obtain user information, that the ThingSmart SDK enforces a secondary confirmation so the key cannot be misused, that the Firebase parameters are public identifiers, and that no rotation is necessary for any of the three. These statements are UNVERIFIED. RFI-IRFOS accepted the MobTech and ThingSmart reasoning in its message of 8 September 2026 and noted that the Firebase answer did not say whether Security Rules, API restrictions and Auth configuration behind eufy-prod-158108 were reviewed.

RFI-IRFOS rates this finding MEDIUM. The first notice rated it CRITICAL on the strength of the ThingSmart secret. Given Anker's statement that the secret cannot be used without a secondary confirmation, and the absence of any test, the rating follows the demonstrated fact, which is that the values are readable.

Impact: Anyone can read these values from the public app. If the ThingSmart secret is sufficient to act against the device-control backend, a third party could build clients that talk to eufy devices. Anker says it is not sufficient. The state of the Firebase project behind the key is not shown.

Fix: State in writing whether the Firebase Security Rules, API restrictions and Auth configuration behind eufy-prod-158108 were reviewed, restrict the key by package name and signing certificate, enforce App Check, and keep the secondary confirmation for ThingSmart documented.

C3: Camera-backend (VSAAS) configuration with a mainland-China endpoint and a Shenzhen storage bucket inside a cleaning app

LOW, 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), reassessed from CRITICAL in the first notice, rated LOW by blast-radius escalation

The dex holds https://vsaas-api-cn-qa.anker.com.cn, https://vsaas-api-ci.eufysecurity.com, https://mysecurity.eufylife.com, https://cn-eufy.oss-cn-shenzhen.aliyuncs.com and https://aiot-clean-api-cn.anker.com.cn, the strings createByVsaas and getPluginFromVSaas, and eight DOMAIN_PLACE_HOLDER categories covering security, pet, baby, health, soundcore and clean brands. The manifest declares 336 activities. No reachable camera screen was found in a resources-only decompile.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to LOW because CVSS gives dormant configuration with no demonstrated exposure 0.0. The finding is rated LOW because it shows that a household cleaning app carries the plumbing of a camera-surveillance backend and a mainland-China endpoint, which is a question of design and data minimisation. CRITICAL, as disclosed on 23 August 2026, is withdrawn because no active path was shown and because Anker states that the code is dormant legacy from discontinued features and that no personal data flows through it.

```
https://mysecurity.eufylife.com
https://mysecurity-qa.eufylife.com
https://vsaas-api-ci.eufysecurity.com
https://vsaas-api-cn-qa.anker.com.cn        mainland-China region, VSAAS = Video
    Surveillance as a Service
https://vsaas-api-qa.eufylife.com
https://vsaas-api-qa.eufysecurity.com
https://security-mall.eufylife.com
https://cn-eufy.oss-cn-shenzhen.aliyuncs.com  Alibaba Cloud object storage, Shenzhen
https://aiot-clean-api-cn.anker.com.cn        this app's own vacuum-control API, China
     region
https://appliances-api-cn-qa.anker.com.cn
createByVsaas
getPluginFromVSaas
```

```
SECURITY_CATEGORY_DOMAIN_PLACE_HOLDER
PROALARM_DOMAIN_PLACE_HOLDER
PRO_MONITOR_DOMAIN_PLACE_HOLDER
PET_CATEGORY_DOMAIN_PLACE_HOLDER
BABY_CATEGORY_DOMAIN_PLACE_HOLDER
SOUNDCORE_CATEGORY_DOMAIN_PLACE_HOLDER
HEALTH_DOMAIN_PLACE_HOLDER
CLEAN_CATEGORY_DOMAIN_PLACE_HOLDER
```

The app under the eufy Clean listing is built from a shared Anker and eufy platform whose code and remote configuration also cover security cameras, pet, baby and health products and the Soundcore brand. The plugin strings indicate a mechanism that could load camera functionality. Whether it is active, dormant or gated by entitlement or region is a runtime question and UNVERIFIED. The 2022 public reporting about eufy camera cloud access is

context only and is not binary evidence for this app.

Anker's reply of 26 August 2026 states that the protocol fields, China domain references and plugin-loading mechanisms are dormant legacy remnants of discontinued video features, that no active execution path or data collection routes personal data through them in this build, and that it is purging them. On 8 September 2026 Anker named EU Standard Contractual Clauses with a Transfer Impact Assessment as the Art. 46 safeguard should that ever change, and committed to completing the removal by the end of October 2026. RFI-IRFOS recorded the question as closed on 8 September 2026. On 18 November 2026 Anker reported: "VSAAS code-path removal - Completed", with the legacy definitions, domain references and dynamic-loading logic removed from the latest public version. This is stated by the operator, not verified by RFI-IRFOS. RFI-IRFOS analysed version 3.19.0 and has not re-analysed a later build, so whether a build after 3.19.0 no longer contains these strings is UNVERIFIED.

Impact: Owners of a cleaning robot do not expect their app to carry the configuration of a camera surveillance service. Anker says nothing flowed through it and that the removal is completed, a statement RFI-IRFOS has not verified against a current build.

Fix: Remove the legacy VSAAS definitions, domain references and dynamic loading logic from the production build, as committed, and confirm the removal and the build number in writing.

H1: MobTech ShareSDK and its consent string for collecting the installed-app list

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 2.1 (CVSS-B), disclosed as HIGH on 23 August 2026, rated LOW in this report

The manifest bundles MobTech ShareSDK (cn.sharesdk.*, com.mob.*) with Mob-AppKey 3504ca74a0820 and an exported LoopShareActivity. The string sharesdk_agreement_dialog_content says that MobTech should have the user's opt-in consent to collect software list information independently and that refusal blocks the related products and services.

```
<meta-data android:name="Mob-AppKey" android:value="3504ca74a0820"/>
<provider android:authorities="com.eufylife.smarthome.com.mob.MobProvider" android:
    name="com.mob.MobProvider"/>
<provider android:authorities="com.eufylife.smarthome.cn.sharesdk.ShareSDKFileProvider
    " android:name="cn.sharesdk.framework.utils.ShareSDKFileProvider"/>
<activity android:exported="true" android:name="cn.sharesdk.loopshare.
    LoopShareActivity">
    <data android:host="cn.sharesdk.loop" android:scheme="ssdk3504ca74a0820"/>
```

```
<string name="sharesdk_agreement_dialog_content">In order to trace the source of your
    closed-loop
sharing function and help you to refine which APP you have shared with one-click or
    logged in via
third-party APP, MobTech should have your active (meaning: opt-in) consent to collect
    your software
list information independently. If you refuse, you will not be able to use the related
     products
and / or services.</string>
```

An installed-app list is a well-known device-fingerprinting input and is not needed to control a vacuum. The consent dialog was not observed at runtime, so whether the gate works as described, and which services refusal blocks, is UNVERIFIED. Anker's reply of 26 August 2026 states that the server-side configuration currently disables collection of the installed-app list (backflow false), that the manifest queries serve local checks such as the availability of share buttons, and that it will remove the redundant permissions, consent strings and collection logic in its next update. This is a vendor statement and is UNVERIFIED. RFI-IRFOS rates the finding LOW because collection was not observed and the vendor reports it as disabled. The consent string is the reason the finding stays in the report.

Impact: Users are told in their own app that a Chinese sharing vendor may collect the list of apps on their phone. If the server flag is off, nothing is collected. The consent text says otherwise, and users who refuse are told that related services stop.

Fix: Remove the MobTech collection code and consent string as announced, and state which functions are blocked on refusal.

H2: Network security configuration permits cleartext traffic for every domain and sets no pinning

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), disclosed as HIGH on 23 August 2026, rated LOW in this report

res/xml/network_security_config.xml holds one base-config with cleartextTrafficPermitted true, no domain-config and no pinning. No cleartext request to the operator's own https endpoints was found in the dex string table.

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true" />
</network-security-config>
```

The configuration does not enforce the https endpoints, and any bundled SDK or later regression could fall back to plain HTTP. RFI-IRFOS rates the finding LOW because no cleartext use was found. Anker's reply of 26 August 2026 confirms the finding, says its primary cloud endpoints require HTTPS and that port 80 is closed, and says it will restrict cleartext traffic globally and add certificate pinning in the upcoming release. Completion is UNVERIFIED because builds after 3.19.0 were not analysed.

Impact: If any request falls back to plain HTTP, a person on the same network could read or change it. No such request was found.

Fix: Set cleartextTrafficPermitted to false, add narrow exceptions only where needed, and add certificate pinning, as committed.

H3: No consent-management platform found, full Firebase suite present, Crashlytics collection enabled

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), added in this report, not itemised in the first notice

The dex holds Firebase analytics, crashlytics, remoteconfig, abt, messaging, installations, iid, measurement, heartbeatinfo, datatransport and dynamicloading, the Google Advertising ID client and the AD_ID permission. firebase_crashlytics_collection_enabled is true. No IAB TCF, OneTrust, Didomi or Usercentrics class was found. No FirebaseInitProvider entry exists in the manifest.

```
<meta-data android:name="firebase_crashlytics_collection_enabled" android:value="true
    "/>
com/google/firebase/*: analytics, crashlytics, remoteconfig, abt, messaging,
    installations, iid, measurement, heartbeatinfo, datatransport, dynamicloading
com.google.android.gms.ads.identifier.AdvertisingIdClient   permission com.google.
    android.gms.permission.AD_ID
```

The manifest has no FirebaseInitProvider with initOrder 100 and directBootAware true, the pattern that forces Firebase to start before any consent screen in two other targets of this programme. This is a structural difference and is credited. Whether Firebase starts early through code in Application.onCreate is UNVERIFIED because no smali pass was run. The finding is that no standards-based consent framework is present while the full Firebase telemetry suite and the advertising ID client are, and Crashlytics collection is left on. The privacy notice does not enumerate the Firebase subsystems or MobTech individually. A declared permission and a library class show capability and not use. RFI-IRFOS rates the finding LOW.

Impact: A user may be measured by crash and analytics services before having been asked. What the app transmits at start-up was not measured.

Fix: Document when each Firebase subsystem starts relative to consent, list the recipients in the privacy notice, and start Crashlytics collection only after consent where it is not strictly necessary.

H4: Self-declared transfers to China and China-headquartered group processors, unnamed

LOW, 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), reassessed from HIGH in the first notice, rated LOW by blast-radius escalation

Anker's privacy notice states that it transfers personal data to other countries including China, the EEA, the UK and the US, that its entities headquartered in China provide global services such as product research, data operations and customer support as intra-group processors, and that there is currently no adequacy decision for China. It names Standard Contractual Clauses only generically where applicable.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to LOW because CVSS gives a disclosed transfer with no technical exposure 0.0. The finding is rated LOW because the operator itself discloses the transfers and the missing adequacy decision, which is candid, and because the open point is which product lines and data the China-based processors touch. HIGH, as disclosed on 23 August 2026, is withdrawn because Anker states in its replies that transfers to China-headquartered group entities are governed by an Intra-Group Data Processing Agreement that incorporates EU Standard Contractual Clauses supported by a Transfer Impact Assessment, and points to Sections 7.1 and 11.2 of its notice. Those statements are UNVERIFIED.

```
"we transfer Personal Data to other countries that may have different laws and data
    protection compliance requirements than those that apply in the country in which
    you are located, including China, the EEA, the UK, and the US."

"these intra-group service providers, acting as Data Processors, include our entities
    headquartered in China that provide global services such as product research, data
     operations, and customer support."

"There is currently no adequacy decision for China; and there is only a partial
    adequacy decision for the U.S."
```

Combined with C3, the practical question is which of the functions performed by China-headquartered entities touch the floorplan, obstacle photo and device-sharing data of C1. The exact in-app consent URL is not hardcoded in the package and is probably loaded from remote configuration, so the general notice, which the app links from its settings string menu_privacy_policy as the Anker Innovations Privacy Notice, is the best available proxy. In its reply of 26 August 2026 Anker accepted the feedback on entity transparency and said an upcoming policy update would name the entities involved. Its reply of 8 September 2026 says it does not currently plan to amend the unified global privacy policy for the People disclosure. Whether the entity clarification is published is UNVERIFIED.

Impact: An EU household's map and obstacle data may be handled by group entities in China. Anker names the legal safeguard it uses. What households cannot see is which entity handles which data.

Fix: Name the China-headquartered entities and the data categories they process in the privacy notice, and state which transfers rest on the Intra-Group Data Processing Agreement and Standard Contractual Clauses.

M1: Play Data Safety label omits location, photos and audio although the permissions are requested

LOW, 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), added in this report, not itemised in the first notice, rated LOW by blast-radius escalation

The app requests ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, CAMERA and RECORD_AUDIO. The Data Safety section read on 23 August 2026 lists device or other IDs, in-app messages, email address, user IDs, phone number and crash logs, and no location, photos and videos or audio category. It also states that no data is shared with third parties.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to LOW because CVSS gives a label discrepancy 0.0. The finding is rated LOW because the camera is demonstrably used for obstacle photos and the donation flow (C1), so a consumer comparing label and permissions sees a mismatch. Google's taxonomy distinguishes sharing from processing by a group or service-provider entity, so the statement that no data is shared is not necessarily wrong.

Impact: A person who reads the label before installing sees no photo or location category although the app can use the camera and, with consent, send photos.

Fix: Align the Data Safety declaration with the permissions and the donation flow.

M2: Exported login activity and exported BLE companion service

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), added in this report, not itemised in the first notice

LoginAuthActivity, CdmBleCompanionService and cn.sharesdk.loopshare.LoopShareActivity are declared exported true. Fifteen components in total carry exported true. Validation inside the components was not examined.

```
<activity android:exported="true" android:name="com.oceanwing.eufyhome.account.login.
    LoginAuthActivity"/>
<service android:exported="true" android:name="com.thingclips.smart.android.common.
    cdmbluetooth.CdmBleCompanionService"/>
<activity android:exported="true" android:name="cn.sharesdk.loopshare.
    LoopShareActivity">
```

Both components can at least be started by another installed app with a matching intent. Impact depends on validation inside each component, which is UNVERIFIED because dynamic testing was not part of this analysis. The finding is a component exposure observation and not a demonstrated exploit.

Impact: A malicious app on the same phone could try to start the login or pairing flow. Whether this changes anything is not shown.

Fix: Set exported to false where no outside caller is needed, or protect the components with signature-level permissions.

M3: android:persistent set to true at application level

LOW, 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), added in this report, not itemised in the first notice, rated LOW by blast-radius escalation

The application tag declares android:persistent true next to android:allowBackup false and the application class com.oceanwing.eufyhome.EufyHomeApplication. A separate monitor process hosts com.thingclips.smart.android.hardware.service DevTransferService and GwBroadcastMonitorService.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to LOW because CVSS gives a manifest attribute with no demonstrated effect 0.0. The finding is rated LOW as a design observation. The attribute is historically reserved for system applications, and modern installs generally ignore it for third-party apps. It signals an intent for always-on background operation, consistent with the monitor process for BLE and gateway broadcasts. No runtime process monitoring was done.

Impact: No effect on users is shown. The attribute indicates a design intent only.

Fix: Remove the attribute if it is not needed, and document the background operation of the monitor process.

Impact Analysis

- People in the robot's view. A child at play, a partner asleep, an elderly relative or a visitor can be photographed, and the account holder can send the capture to eufy (C1).
- Households with a robot. A room map is held under a cloud map ID and can be shared with a second account (C1).
- Users of the share function. A MobTech consent string describes collection of the installed-app list on the phone (H1).
- EU users. Group entities in China act as processors and no adequacy decision exists. Anker names SCCs with a TIA as the safeguard (H4).
- All users. Credentials in the package, permissive cleartext configuration, camera-backend plumbing and telemetry without a consent framework form the background (C2, C3, H2, H3).

The Complete Chain

- 1. A household installs eufy Clean and enables Real Obstacle Photos.
- 2. The robot photographs obstacles. The taxonomy includes People, Pets and Poop.
- 3. The app shows the photo to the account holder, who can donate the capture and a device log to eufy for algorithm improvement.
- 4. According to Anker the capture is de-identified on the device before transmission. That is UNVERIFIED.
- 5. The room map is stored under a cloud map ID and the device can be shared with a second account.
- 6. Group entities in several countries, among them China-headquartered processors, handle data under an intra-group agreement with SCCs, according to Anker.

Each later section refers to one of these links. The harm is that a photograph of a person is part of an ordinary product function, decided by someone else, with disclosure only at the account holder's consent screen.

People in the Photo & Bystanders

A robot with a camera at floor level sees whoever is on the floor. In a household that is disproportionately a child at play, a person asleep or an elderly relative. Art. 13 and Art. 14 require information for people whose data is processed, and a bystander has no account through which a notice could reach them. Whether the donated capture relates to an identifiable person at all depends on the de-identification that Anker describes. If the de-identification is irreversible and runs before classification, the privacy impact is considerably smaller. Anker was asked for the test or audit that establishes the order of the steps and has not provided one, including in its reply of 18 November 2026, which states that the masking is irreversible. The three standards it named are certifications of management systems and are not a DPIA.

This report does not rely on Art. 9 GDPR. An image of a person becomes biometric data only when processed to identify them, and Anker states that this is not the purpose. The household exemption of Art. 2(2)(c) may cover the account holder's own use and does not decide the operator's position, because the operator designed the donation flow. Anker's position that the account holder's consent activates the feature and that no separate bystander basis is required stands on its de-identification claim.

Data Protection: Article by Article

Article	How it is engaged
Art. 5(1)(a)	Transparency. People category and donation flow not named in the privacy notice (C1).
Art. 5(1)(c)	Data minimization. A People category and the installed-app list for an obstacle-avoidance and control app (C1, H1).
Art. 6(1)(a)	Basis stated by Anker for the donation flow, the account holder's consent (C1).
Art. 7(1), Art. 7(4)	Consent timing and coupling of services to the MobTech consent (H1, H3).
Art. 13(1)(c), (e)	Purposes and recipients. Donation purpose and recipient as a distinct activity (C1), Firebase and MobTech recipients (H3).
Art. 13(1)(f)	Transfer safeguards. Generic reference to SCCs in the notice (H4).
Art. 25	Data protection by design. Dormant camera plumbing (C3), exported components (M2), persistent flag (M3).
Art. 28	Processors. Tuya and MobTech as platform processors (C2), China-headquartered intra-group processors (H4).
Art. 32(1)(a), (b)	Security of processing. Credentials (C2), cleartext (H2), exported components (M2).
Art. 35	DPIA for photographing people in a home. Anker states on 18 November 2026 that one was conducted; the document was not provided and the statement is stated by the operator, not verified by RFI-IRFOS (C1).
Art. 44, Art. 46	Transfers to China. SCCs with TIA named by Anker (C3, H4).

Regulatory & Legal Landscape

Anker's privacy notice lists joint controllers in the United States, Germany, the Netherlands and Hong Kong without a designated lead, so this report assumes no lead authority. The Datenschutzbehörde and the EDPS were informed for transparency. Research on the published package is protected by Art. 17 StGG and follows ISO/IEC 29147.

Industry comparison: Anker discloses camera-based navigation and home-environment data in its notice in general terms, admits China-headquartered processing and the lack of an adequacy decision, uses opt-in framing for Real Obstacle Photos and donation, and answered in writing twice. Placing the disclosure at the point of consent, as Anker proposes, serves the account holder. It does not reach the person in the photo.

Indicators of Compromise & Reproducible Evidence

Every point below can be reproduced from the public package and the public web pages. The package was obtained from the APKPure mirror because the audit device was not reachable on the analysis day. Its version code matched the live Google Play listing and its content length of 144,648,007 bytes matched the archived file.

```
Package       com.eufylife.smarthome (Play title eufy Clean(EufyHome), developer Anker
    )
Version       3.19.0 / versionCode 1040
APK           144,648,007 bytes (137.9 MB), SHA-256
    db716d3e9402e5fb87fad40a57230489e29decf8e83eafa4d258b942e0449515
SDK           minSdkVersion 24, targetSdkVersion 35
Dex           15 classes*.dex, about 6,087 unique class-descriptor strings
Namespace     com.oceanwing.eufyhome, launch activity com.oceanwing.eufyhome.main.
    WelcomeActivity
```

```
THING_SMART_APPKEY   fdkdn5hpmujkvpfgv3pc
THING_SMART_SECRET   3w38pdhqyqtrcv3y898ytqwt85katjgg
Mob-AppKey           3504ca74a0820
Mob-AppSecret        77797af3d4cbfab0d474e53a914e5312
Firebase API key     AIzaSyDTSD_9xTfo3bTuOCmEatTp-lGbFmm7wsA
Firebase app ID      1:466383759367:android:f4f9c96472b0e050
Project ID           eufy-prod-158108
Database URL         https://eufy-prod-158108.firebaseio.com
Storage bucket       eufy-prod-158108.appspot.com
Web client ID        466383759367-3c35hr3r2bb1433ijr5a84v3ch8scpc1.apps.
    googleusercontent.com
Privacy notice       https://www.eufy.com/pages/privacy-policy (Anker Group privacy
    notice, menu_privacy_policy)
```

```
DPO@anker.com           data protection contact, sender of the replies
support@eufylife.com     support contact
support@anker.com        general support
Ticket ANKER-TNC1054839961   eufy Customer Support
```

Disclosure Timeline & Outcome

Date	Event
2026-08-23	Analysis of version 3.19.0. Notice REF EUFYCLEAN-2026-R1 sent to DPO@anker.com and support@eufylife.com, copied to the Datenschutzbehörde and the EDPS. Six findings itemised and three written questions.
2026-08-24	Acknowledgment from eufy Customer Support (ticket ANKER-TNC1054839961). The request was forwarded for internal review.
2026-08-26	First substantive reply from Anker. On-device de-identification of people, credentials described as vendor-mandated integration artifacts with an engineering review, VSAAS code described as dormant legacy and being purged, MobTech list collection disabled server-side, cleartext confirmed with restriction and pinning announced, SCCs with TIA for China transfers, no evidence of a breach under Art. 33(4).
2026-08-26	RFI-IRFOS replies that each of the three questions was answered on one half. Open: naming the People category and donation flow in the policy, the audit behind the de-identification claim, a dated rotation plan for the credentials and Firebase key, and the Art. 46 safeguard for a reactivated VSAAS path.
2026-08-27	Acknowledgment. Anker asks for test reports or screenshots.
2026-09-08	Second substantive reply. In-app disclosure to be enhanced and VSAAS removal to be completed by the end of October 2026, privacy policy not to be amended for the People disclosure, no rotation for MobTech, ThingSmart or Firebase, SCCs with TIA named as the Art. 46 safeguard.
2026-09-08	RFI-IRFOS records the VSAAS question as closed and the MobTech and ThingSmart answers as accepted. Three points open with a deadline of 22 September 2026: the DPIA, the bystander, and the review of Security Rules, API restrictions and Auth configuration behind eufy-prod-158108.
2026-09-09	Acknowledgment. The points were forwarded to the relevant internal team, with an answer promised before the deadline.
2026-11-15	RFI-IRFOS sends a notice to Anker stating publication for 21 November 2026.
2026-11-18	Third substantive reply from Anker (ticket ANKER-TNC1054839961). DPIA stated to exist, faces and human forms stated to be irreversibly masked on the device, Firebase project reviewed with both keys bound to the package name and signing certificate, VSAAS removal reported completed, in-app disclosure scheduled for the end of November 2026. Statements stated by the operator, not verified by RFI-IRFOS.
2026-11-21	Embargo reached. This report is published.

The operator received the same embargo date in every message. No request to extend it was made and none was granted. The three points asked on 8 September 2026 were answered on 18 November 2026, 71 days later and 3 days before publication. The end-of-October commitments were reported on that date as completed for the VSAAS removal and the Firebase restrictions, and as rescheduled to the end of November 2026 for the in-app disclosure.

What Anker Got Right

- Anker answered in writing twice, within three days of the notice and again on 8 September 2026, and committed to dated remediation.
- The privacy notice discloses camera-based navigation and home-environment data in general terms, a better starting position than the other robot vacuum in this wave.
- The notice is candid about China-headquartered group processors and the missing adequacy decision.
- Real Obstacle Photos and the donation flow are opt-in and not on by default.
- No FirebaseInitProvider with initOrder 100 and directBootAware true is present, which avoids the structural pre-consent start found in two other targets.
- allowBackup is false, so app data is excluded from Android automatic cloud backup.
- Anker confirmed the cleartext finding, announced restriction and pinning, and announced removal of the VSAAS code and the MobTech collection logic.
- The app targets API 35 and is actively maintained.

Residual Risk & Recommendations

All ten findings are rated as audited. Anker reported on 18 November 2026 that the VSAAS removal and the Firebase key restrictions are completed and that the enhanced in-app disclosure is scheduled for the end of November 2026, and has announced cleartext restriction, pinning and removal of the MobTech collection logic without a date. None of this has been verified by RFI-IRFOS, and builds after 3.19.0 were not analysed. The DPIA exists according to Anker but was not provided, and the bystander transparency rests on the announced disclosure.

- Publish the DPIA conclusion for photographing people in a home and the audit that shows de-identification precedes classification, and name the People category and donation flow in the privacy policy.
- State how Art. 13 and Art. 14 information reaches the person in a donated photo who is not the account holder.
- Confirm in writing the review of Security Rules, API restrictions and Auth configuration behind eufy-prod-158108, and enforce App Check.
- Confirm the removal of the VSAAS definitions and the MobTech collection logic with the build number, and name the China-headquartered entities and the data they process.
- Block cleartext traffic and add pinning as announced, and protect the exported components.
- Align the Data Safety label with the permissions and the donation flow.

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 the operator’s public privacy notice and Google Play listing. No Anker servers or accounts were probed and no key was tested. Severity per CVSS v4.0 (CVSS-B) with explicit blast-radius escalation where stated. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF EUFYCLEAN-2026-R1.