Security & Privacy Disclosure, Final Report

Roborock for Android (com.roborock.smart)

A labelled 3D model of your home and a pet-photo upload, that the public privacy policy never mentions.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. THE OPERATOR REPLIED ON 31 AUGUST AND ON 20 NOVEMBER 2026 AND ANSWERED THE THREE QUESTIONS. ITS STATEMENTS ARE NOT VERIFIED BY RFI-IRFOS.

Target	Beijing Roborock Technology Co., Ltd., Room 1001, Floor 10, Building 3, Yard 17, Anju Road, Changping District, Beijing, P.R. China
Versions Audited	4.72.02 / versionCode 100920 (analysed 2026-08-23), 70.5 MB, Google Play update of 2026-08-07
Supervisory Authority	Datenschutzbehörde, Austria, informed for transparency. The operator is established in China and names Roborock Germany GmbH, Düsseldorf, as its GDPR representative (stated by the operator on 20 November 2026, UNVERIFIED). No lead authority is assumed.
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	10: 1 High, 4 Medium, 5 Low (seven from the first notice, re-assessed, and three added)
Status	REPLIES OF 31 AUGUST AND 20 NOVEMBER 2026. THE REPLY OF 20 NOVEMBER 2026 ANSWERS THE THREE QUESTIONS AND STATES CHANGES IN THE LATEST VERSION, WHICH RFI-IRFOS HAS NOT VERIFIED.
SHA-256 (base APK)	`a22037efa3113a6a9f2c05acf19b5a3fd1e87c12a1ac650e4ec9a698f8c8af0a`

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: Labelled 3D home and pet model, pet-photo upload and cross-account room-map sharing, absent from the public privacy policy . . . 8

5.2 C2: Hardcoded client credentials in the manifest and resources, including an IoT SDK appkey and appsecret . . . 10

5.3 C3: Firebase provider initializes before any consent screen can render . . . 11

5.4 H1: Self-declared storage in China, Germany and the United States, with the transfer mechanism and EU representative not shown . . . 12

5.5 H2: Network security configuration permits cleartext traffic for every domain and sets no pinning . . . 13

5.6 H3: Live audio and video remote viewing can capture people who are not the account holder . . . 14

5.7 H4: Meta Protected Audience code and the full Privacy Sandbox permission set in a device-control app . . . 15

5.8 M1: Exported FCM message service . . . 16

5.9 M2: Test and staging hostnames in the production build . . . 16

5.10 M3: Location permissions declared, location absent from the Play Data Safety list of collected data . . . 17

6 Impact Analysis 17

7 The Complete Chain 18

8 Home Mapping, Pets & Bystanders 18

9 Data Protection: Article by Article 19

10 Regulatory & Legal Landscape 20

11 Indicators of Compromise & Reproducible Evidence 20

12 Disclosure Timeline & Outcome 21

13 What Roborock Got Right 22

14 Residual Risk & Recommendations 22

Executive Summary

Roborock is the control app for Roborock robot vacuums, lawn mowers, wet and dry vacuums and washer-dryers. It is published on Google Play by Beijing Roborock Technology Co., Ltd. with more than 10 million downloads. On 23 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF ROBOROCK-2026-R1 after a root level code analysis of version 4.72.02. The notice itemised seven findings, three Critical and four High, and asked three written questions.

The case turns on what a camera and lidar robot knows about a home. The package ships a labelled library of 3D furniture and pet models (sofas, beds, toilets, mirrors, a cat bed, a litter tray, a cat cage, a dog), a bundled Caffe object-detection model with native OpenCV, a room and map data model that stores room names, map ID and floor type, a working device-sharing feature that lets a second account read the room structure of a map (getShareDeviceRooms) and a Pet AI plugin whose identifiers describe a cloud upload of pet photos and video (getPetUploadURL) behind its own consent flag (hasPetPhotoAgreements). The general public privacy policy retrieved on 23 August 2026 contains none of the words map, photo, image, video or recognition.

Roborock replied on 31 August 2026 that these features are disclosed in the respective device privacy policies, which users see after network configuration. That document is not part of the evidence, so the statement is UNVERIFIED. The same policy admits storage in data centers in China, Germany and the United States and limited remote access by group entities outside the user's country. A live audio and video remote-viewing feature, a client key set including an IoT command-API appkey and appsecret, a Firebase provider that starts before any consent screen, and Meta advertising code with the full Privacy Sandbox permission set complete the picture.

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

Roborock's reply of 31 August 2026 says the findings are false positives of an automated scanning tool, which is not how the analysis was done, and that other issues are being studied. RFI-IRFOS answered on 3 September 2026, accepted the Firebase point as within vendor guidance and restated three questions with a deadline of 17 September 2026. A reminder of 15 November 2026 named 21 November 2026 as the publication date. On 20 November 2026, 78 days after the follow-up, Roborock replied from privacy@roborock.com. The reply answers the three questions, names Roborock Germany GmbH in Düsseldorf as its GDPR representative and states for the latest version, without naming a version number, that the IoT SDK appsecret is removed from the client code, that Firebase initialises after the consent screen, that only HTTPS connections are permitted and that the Meta advertising permission group is gone. These are statements by the operator and RFI-IRFOS has not checked them against a current build. The findings below describe version 4.72.02 and keep their severities. The report is published on 21 November 2026, 90 days after delivery.

Scope: Root level code analysis of Roborock 4.72.02 (versionCode 100920): AndroidManifest.xml, decoded resources, five classes dex files with about 36,200 unique class-descriptor strings, bundled assets, the React Native bundle of the Pet AI plugin and the native library list. 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 (uploaded 2026-08-08) after version and size matched the live Google Play listing, because the audit device was not reachable on the analysis day. The operator's general privacy policy at global.roborock.com/pages/privacy-policy (about 28,000 characters) and the public Google Play listing were read on 23 August 2026. The device privacy policies that Roborock names in its replies, among them the one linked on 20 November 2026, were not read. No account was created, no Roborock server was called, no key was tested and no runtime instrumentation was used. 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	Labelled 3D home and pet model, pet-photo upload and cross-account room-map sharing, absent from the public privacy policy
C2	MEDIUM	Hardcoded client credentials in the manifest and resources, including an IoT SDK appkey and appsecret
C3	MEDIUM	Firebase provider initializes before any consent screen can render
H1	MEDIUM	Self-declared storage in China, Germany and the United States, with the transfer mechanism and EU representative not shown
H2	LOW	Network security configuration permits cleartext traffic for every domain and sets no pinning
H3	MEDIUM	Live audio and video remote viewing can capture people who are not the account holder
H4	LOW	Meta Protected Audience code and the full Privacy Sandbox permission set in a device-control app
M1	LOW	Exported FCM message service
M2	LOW	Test and staging hostnames in the production build
M3	LOW	Location permissions declared, location absent from the Play Data Safety list of collected data

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	HIGH	Notice finding 1. Reply of 20 November names one device privacy policy and states full disclosure there. Not verified. Reassessed.
C2	CRITICAL	MEDIUM	Notice finding 2. Reply of 20 November: Maps key restricted, appsecret removed from the client code in the latest version. Stated, not verified. Reassessed.
C3	CRITICAL	MEDIUM	Notice finding 3. Reply of 20 November: Firebase starts after the consent screen in the latest version. Stated, not verified. Reassessed.
H1	HIGH	MEDIUM	Notice finding 4. Reply of 20 November names Roborock Germany GmbH as representative, storage in Germany and SCC or adequacy for transfers. Stated, not verified. Reassessed.
H2	HIGH	LOW	Notice finding 5. Reply of 20 November: HTTPS only in the latest version. Stated, not verified. Reassessed.
H3	HIGH	MEDIUM	Notice finding 6. Reply of 20 November: Roborock is not the data controller of the stream and the Data Safety audio and video categories are checked. Stated, not verified. DPIA question not addressed. Reassessed.
H4	HIGH	LOW	Notice finding 7. Reply of 20 November: the Meta advertising permission group is absent in the latest version. Stated, not verified. Reassessed.
M1	Not itemised	LOW	Added in this report. Reply of 20 November calls the service a standard Firebase Cloud Messaging component.
M2	Not itemised	LOW	Added in this report. Reply of 20 November: unused domains carry no business logic and have no impact on users. Stated, not verified.
M3	Not itemised	LOW	Added in this report. Reply of 20 November: the location category is checked and disclosed in Data Safety. Stated, not verified.

Subject & Operator Analysis

Roborock (package com.roborock.smart) is published on Google Play under the developer name Roborock. On 23 August 2026 the listing showed more than 10 million downloads and an update on 7 August 2026. The content rating is PEGI 3 on Google Play and on APKPure. The app controls robot vacuums, lawn mowers, wet and dry vacuums and washer-dryers.

The operator is Beijing Roborock Technology Co., Ltd., Room 1001, Floor 10, Building 3, Yard 17, Anju Road, Changping District, Beijing. The entity is confirmed by the Beijing ICP filing embedded in res/values/strings.xml and by the operator's own privacy policy, which names it as Personal Information Handler. The privacy contacts are privacy@roborock.com, privacy@roborock-eu.com and dpo@roborock.com. support@roborock-eu.com was also found for EU-routed support.

The package targets Android API 35 with minSdkVersion 24 and ships five classes dex files with about 36,200 unique class-descriptor strings. Roborock states that its App Privacy Policy names an EU representative in Germany. That statement is UNVERIFIED.

Architecture & Data Flow

- App to robot through the manufacturer's cloud. Region-partitioned endpoint families (api, iot and wood hosts with -eu, -us, -cn and -ru variants) are in the package.
- Map and room model on the device side: RN3DMapNewActivity and the mapv2 classes store roomName, mapId and floorType and render furniture from the bundled g3db library.
- Object detection: a bundled Caffe model with a super-resolution pair and native OpenCV. Where inference runs is UNVERIFIED.
- Pet AI plugin: a React Native feature with a pet upload URL, per-device pet photo authorizations and an agreement flag that is separate from the general agreement.
- Device sharing: acceptShareDevice, removeShareDevice and getShareDeviceRooms give a second account access to the room structure.
- Remote viewing: a WebRTC call flow with ICE configuration. Per the operator the stream is relayed under certain network conditions and not stored (vendor statement, UNVERIFIED).
- Third-party SDKs: Firebase (Crashlytics collection disabled), Facebook SDK (auto logging and advertiser ID collection disabled) and Privacy Sandbox advertising classes.

The architecture is that of a modern camera and lidar robot. The risks sit in how much of the home model leaves the device, who can read it and how clearly the policy says so.

Findings

C1: Labelled 3D home and pet model, pet-photo upload and cross-account room-map sharing, absent from the public privacy policy

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

The package contains 3D models of sofas, beds, toilets, mirrors, cabinets, a cat, cat bed, cat litter tray, cat cage and dog, a Caffe object-detection model (detect.caffemodel and detect.prototxt) with a super-resolution pair, native OpenCV, a room and map data model, a device-sharing subsystem with getShareDeviceRooms and a Pet AI plugin with getPetUploadURL and hasPetPhotoAgreements. The general privacy policy retrieved on 23 August 2026 contains none of the words map, photo, image, video or recognition.

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 data describes the inside of a private home, the rooms, the furniture that tells a bedroom from a bathroom and whether a household keeps a cat or a dog, because a second account can be given the room structure, because the people recorded can include persons who are not the account holder, and because the app has more than 10 million downloads. CRITICAL, as disclosed on 23 August 2026, is withdrawn because the payload of the upload, the retention period and whether recognition runs on the device or on a server were not observed, and because Roborock states that device privacy policies cover these features.

```
sofa1.g3db sofa2.g3db sofa3.g3db sofaLL.g3db sofaLR.g3db
bed1.g3db bed2.g3db bedCabinet.g3db
open_toilet.g3db close_toilet.g3db
tall_mirror.g3db tvCabinet.g3db shoesCabinet.g3db clothesCabinet.g3db
cat.g3db cat_bed.g3db cat_cage.g3db cat_plate.g3db dog.g3db
table.g3db weight.g3db charger.g3db robot.g3db chaji.g3db chajiRect.g3db
general.g3db zhiwu.g3db coral_robot.g3db poqi.g3db baba.g3db xian.g3db
u.g3db dizuo.g3db shoes.g3db chapai.g3db
```

```
assets/qrml_models/detect.caffemodel   detect.prototxt
assets/qrml_models/sr.caffemodel       sr.prototxt   (super-resolution)
lib/arm64-v8a/libopencv_java4.so
```

```
AIImageVideoPetEventCollector
getPetUploadURL
checkEnablePetRecognize / enablePetRecognizeIds
authorizedPetPhotoDevices / hasPetPhotoAgreements
fetchMapObstaclePetIds
fetchPatrolTaskPetIds
checkSmartAssistantPetPhotoOpenedDevices
petType, getPetType
```

```
com/roborock/smart/react/map/RN3DMapNewActivity
com/roborock/smart/react/mapv2/view/RR3DMapView
com/roborock/smart/react/mapv2/model/data/RoomBaseColorLevel
com/roborock/smart/react/mapv2/model/data/MapMode
roomName
mapId
floorType

isShareDevice
acceptShareDevice
rejectShareDevice
removeShareDevice
getShareDeviceRooms
```

What the evidence shows: a labelled object library, a bundled detector, a Pet AI plugin whose own identifiers describe a cloud upload gated by a feature-specific agreement flag, a stored room model and a sharing feature that reaches the room structure. What it does not show: the fields transmitted, the retention period, whether recognition runs on the device with the bundled model or on a server, and whether people in frame are excluded from what is captured or uploaded. Code paths found are named for pets, and a camera-based scan does not select what enters the frame.

Policy and code: the general policy at global.roborock.com/pages/privacy-policy, read on 23 August 2026, describes generic categories such as device-related information, usage data and crash data. It does not mention a spatial model of the home, object or pet recognition, or device sharing of that data. Roborock's reply of 31 August 2026 states that the features are fully disclosed in the respective device privacy policies, accessible after the device network configuration is complete. RFI-IRFOS has not seen those documents, and the URL that the in-app agreement screens link to is not hardcoded in the package. On 3 September 2026 RFI-IRFOS asked which policy at which URL discloses the 3D model, the pet recognition and the map sharing. On 20 November 2026 Roborock answered that the privacy notices for these features are fully disclosed in the privacy policies of the respective devices, which become accessible after the user binds the device, that the applicable policy depends on the device model, and it linked one device policy at files.roborock.com as an example. That document was not read for this report, so whether a device policy covers the 3D model, the pet recognition and the map sharing is UNVERIFIED.

Impact: A household that owns a Roborock robot has a room-by-room model of its home held by a company in Beijing. The model says which rooms exist and what furniture is in them, and whether the family has a cat or a dog. A family member, a guest or a former partner with share access can read the room structure. A user who never saw a notice cannot exercise access rights over data they did not know existed.

Fix: Name the home map, object and pet recognition and device-sharing data in the public privacy policy that precedes purchase, state whether recognition runs on the device or on a server and how long photos, video and maps are kept, and publish the DPIA conclusion for this processing.

C2: Hardcoded client credentials in the manifest and resources, including an IoT SDK appkey and appsecret

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 com.roborock.iotsdk.appkey rr, com.roborock.iotsdk.appsecret qWKYcdQWrbm9hPqe and a Google Maps key. res/values/strings.xml carries a Firebase API key, Firebase app ID, database URL rockhome-19f56 and a Facebook App ID with a client token. All values are extractable with apktool from any Play Store download. The functional scope of the appsecret is UNVERIFIED.

```
<!-- AndroidManifest.xml -->
<meta-data android:name="com.roborock.iotsdk.appkey" android:value="rr"/>
<meta-data android:name="com.roborock.iotsdk.appsecret" android:value="
    qWKYcdQWrbm9hPqe"/>
<meta-data android:name="com.google.android.geo.API_KEY" android:value="
    AIzaSyCgKxQATp2aEyz9RoyTLPx0wCgNQsriF08"/>

<!-- res/values/strings.xml -->
<string name="google_api_key">AIzaSyBg_AMeuFMLc7Z9Oy-UXOWXYTthWl2pICM</string>
<string name="google_app_id">1:196751334623:android:576b846efcb16772</string>
<string name="firebase_database_url">https://rockhome-19f56.firebaseio.com</string>
<string name="project_id">rockhome-19f56</string>
<string name="facebook_app_id">554874373514387</string>
<string name="facebook_client_token">07c7262b04c7cece2a4ecc43e525b324</string>
```

The pair appkey and appsecret has the naming of an API authentication pair and may sign requests to the IoT command backend. That is an inference from naming. No credential was used against any server and the functional scope of the appsecret is UNVERIFIED. Firebase client keys are not secrets by Google's design and RFI-IRFOS accepted that point in its follow-up. Roborock states that the Google Maps key is restricted by package name and SHA-1 fingerprint (31 August 2026), and by package name, signing fingerprint and IP in the management console (20 November 2026). That statement is UNVERIFIED. On 20 November 2026 Roborock also stated that the IoT SDK appsecret has been removed from the client code, without naming the version. RFI-IRFOS analysed no later build, so this is stated by the operator and not verified by RFI-IRFOS. The Facebook App ID and client token are client identifiers by design. The one item that is not obviously a public client identifier is the appsecret, which is identical in every installation.

RFI-IRFOS rates this finding MEDIUM. The first notice rated it CRITICAL on the strength of the appsecret naming. A shared secret that is identical in every installation identifies the application and not the user, and nothing shows that it authorizes commands to a device.

Impact: Anyone can read these values from the public app. If the appsecret signs requests to the command backend, a third party could build clients that impersonate the Roborock app. For owners of a robot that moves around their home this would be a matter of trust in the device channel. That outcome is not demonstrated.

Fix: Confirm in writing what the appkey and appsecret authorize and move any real secret out of the client, show the restriction of the Google Maps key, and enforce App Check for the Firebase project rockhome-19f56.

C3: Firebase provider initializes before any consent screen can render

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

FirebaseInitProvider is declared with initOrder 100 and directBootAware true. ComponentDiscoveryService registers the Analytics connector and Sessions registrars unconditionally. Crashlytics collection is disabled by firebase_crashlytics_collection_enabled false, and no equivalent flag exists for Analytics. The app has its own separately worded opt-in for a User Experience Improvement Program.

```
<provider android:authorities="com.roborock.smart.firebaseinitprovider"
    android:directBootAware="true" android:exported="false"
    android:initOrder="100" android:name="com.google.firebase.provider.
    FirebaseInitProvider"/>
<service android:directBootAware="true" android:exported="false"
    android:name="com.google.firebase.components.ComponentDiscoveryService">
    ... AnalyticsConnectorRegistrar, FirebaseSessionsRegistrar, + Crashlytics,
    Installations, Messaging, DataTransport registrars
</service>
<meta-data android:name="firebase_crashlytics_collection_enabled" android:value="false
    "/>
```

```
u_roborock_analytics_service_alert_content: "...information regarding your device,
    using habits, configuration settings, and statistically recorded special events
    will be collected and sent to our server..."
```

A ContentProvider starts when the process binds, before any activity such as AgreementActivity can show a consent screen. Whether Firebase Analytics collects data before the user answers the dialog is a call-order question that the string pool cannot decide and is UNVERIFIED. The same manifest pattern is a Firebase default. RFI-IRFOS therefore rates the finding MEDIUM, in line with the treatment of the same pattern elsewhere in the programme. The finding was not mentioned in Roborock's reply and was raised again on 3 September 2026. On 20 November 2026 Roborock stated that in the latest version Firebase initialisation takes place after the user consent screen is rendered. The version is not named and RFI-IRFOS has not verified the statement.

Impact: A person who installs the app and has not yet answered the consent dialog may already be known to the analytics service. What start-up transmits was not measured.

Fix: Disable automatic Firebase initialization in the manifest, start the SDK after the consent state is known, and state which events the User Experience Improvement Program adds.

H1: Self-declared storage in China, Germany and the United States, with the transfer mechanism and EU representative not shown

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

The operator's general privacy policy states: We store the personal information collected in data centers in China, Germany and the United States. Certain entities in our corporate group that are located outside of your country of residence are granted limited remote access to the above information so that they can provide certain functions. The retrieved text names no Art. 46 mechanism and no Art. 27 representative. It lists dpo@roborock.com and privacy@roborock-eu.com.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because CVSS gives a transfer question with no technical exposure 0.0. The finding is rated MEDIUM because the data in question can include a labelled model of a home (C1) and because storage in China is stated by the operator itself. HIGH, as disclosed on 23 August 2026, is withdrawn because Roborock states in its reply that its App Privacy Policy names an EU representative in Germany and explains the transfer mechanism, and RFI-IRFOS has not been able to read that document.

```
"We store the personal information collected in data centers in China, Germany and the
     United States. Certain entities in our corporate group that are located outside
    of your country of residence are granted limited remote access to the above
    information so that they can provide certain functions."

"Personal Information Handler: Beijing Roborock Technology Co., Ltd. Address: Room
    1001, Floor 10, Building 3, Yard 17, Anju Road, Changping District, Beijing, P.R.
    China. Email: privacy@roborock.com or privacy@roborock-eu.com (for users from
    European Economic Area) ... you may also contact our DPO by sending an email to
    dpo@roborock.com"
```

The exact policy URL that the in-app agreement screens link to is not hardcoded in the package and is very likely loaded at runtime. The general public policy was used as the best available proxy, which is a limitation. A privacy mailbox and a DPO mailbox are not the same as a named Art. 27 representative. Roborock's reply of 31 August 2026 asserts that a representative in Germany and a transfer mechanism are in the App Privacy Policy on the Google Play listing, without naming either in the reply. That statement is UNVERIFIED. The follow-up of 3 September 2026 asked which Art. 46 mechanism covers the transfer to China and for the name and contact address of the representative. On 20 November 2026 Roborock answered that data of European users is stored on servers in Germany, that transfers outside the EEA, the United Kingdom and Switzerland rely on adequacy decisions and Standard Contractual Clauses, and that Roborock Germany GmbH, Peter-Müller-Strasse 16/16a, 40468 Düsseldorf (privacy@roborock-eu.com), is its GDPR representative, both to be found in its App privacy policy. These statements come from the operator and are not verified by RFI-IRFOS.

Impact: An EU household that uses the app may have its map and pet data stored in or accessed from China. Whether the legal safeguards that Chapter V of the GDPR requires are in place is the open question.

Fix: Name the Art. 46 mechanism for each storage location, name the Art. 27 representative

with address in the privacy policy shown before first use, and state which data categories are stored in which country.

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_online.xml, the file the manifest references, holds one base-config with cleartextTrafficPermitted true, no domain-config and no pinning. Every endpoint literal found in the dex is https, so no cleartext request to the operator's backend was found.

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

```
https://api-eu.roborock.com   https://euiot.roborock.com   https://wood-eu.roborock.
    com:8010
and the -cn, -us and -ru counterparts of each family
```

The configuration does not enforce the https endpoints. A third-party SDK, a faulty request builder or a later regression could fall back to plain HTTP without the platform blocking it. RFI-IRFOS rates the finding LOW because no cleartext use was found, in line with the treatment of the same pattern elsewhere in the programme when no cleartext request was shown. On 20 November 2026 Roborock stated that the latest version uses a network security configuration that permits encrypted (HTTPS) connections only. The version is not named and RFI-IRFOS has not checked the statement.

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 in the base configuration, add domain-specific exceptions only where needed, and consider pinning for the control hosts.

H3: Live audio and video remote viewing can capture people who are not the account holder

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

The manifest requests RECORD_AUDIO and CAMERA. The Play permission text reads: Microphone (Optional) Used for sound transmission on devices that support remote viewing. The package contains libjingle_peerconnection_so.so and the strings startCall, remote_control and Please set iceConfigs to nonnull before startCall, which are WebRTC signalling terms. The Play Data Safety label read on 23 August 2026 lists no audio or video category.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because CVSS gives a documented opt-in feature with no demonstrated exposure 0.0. The finding is rated MEDIUM because a camera and microphone that move through a home capture whoever is present, among them partners, children, visitors and cleaners, who made no decision to be recorded. HIGH, as disclosed on 23 August 2026, is withdrawn because the feature is a documented and optional remote-viewing function and the operator states that the stream is not stored and that the device shows a visual indicator and plays an audio alert during recording.

```
uses-permission: android.permission.RECORD_AUDIO
uses-permission: android.permission.CAMERA
lib/arm64-v8a/libjingle_peerconnection_so.so
startCall
remote_control
Please set iceConfigs to nonnull before startCall
```

The audio feature is a named, conventional function and not hidden acoustic sensing. The privacy-relevant point is who it exposes. The app has a separate agreement flag for uploading pet photos (C1) and no equivalent gate for a human in frame was found in the package. Roborock's reply of 31 August 2026 states that the video stream is not stored in any way, that encrypted video data is relayed through the server only under certain network conditions, that Roborock cannot access or store the stream, that the policy obliges users not to record others without authorization, and that the robot has a visual indicator and an audio alert. These statements are vendor statements and are UNVERIFIED. The reply did not say whether a DPIA was carried out or what consent gate applies to a bystander. A device indicator is notice and not consent. On 20 November 2026 Roborock added that it is not the data controller of the video stream for this feature, that it has put adequate security safeguards in place and provided usage reminders to users, and that the audio and video categories have been checked and disclosed in the Google Play Data Safety section. The reply does not say whether a DPIA exists. These statements are the operator's and are not verified by RFI-IRFOS.

Art. 9 GDPR is not relied on in this report. An image or a voice becomes special category data only under conditions that this analysis did not examine. Art. 35 is engaged by the question whether a DPIA exists for the capture of bystanders.

Impact: A partner, a child, a visiting relative or a cleaner in a room where the robot has a live camera and microphone can be seen and heard by the account holder without having been asked. The household member who is recorded is not the person who agreed to the feature.

Fix: Publish the DPIA conclusion for remote viewing, state the consent or notice basis for people in view, show the Data Safety audio and video categories honestly, and describe the indicator behaviour in the policy.

H4: Meta Protected Audience code and the full Privacy Sandbox permission set in a device-control app

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), disclosed as HIGH on 23 August 2026, rated LOW in this report

The manifest requests ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_CUSTOM_AUDIENCE and ACCESS_ADSERVICES_TOPICS. The dex contains com.facebook.appevents.gps.pa.PACustomAudienceClient with CustomAudienceManager and joinCustomAudience calls. The Facebook SDK flags AutoLogAppEventsEnabled and AdvertiserIDCollectionEnabled are set to false. Execution at runtime was not observed.

```
<meta-data android:name="com.facebook.sdk.ApplicationId" android:value="@string/
    facebook_app_id"/>
<meta-data android:name="com.facebook.sdk.ClientToken" android:value="@string/
    facebook_client_token"/>
<meta-data android:name="com.facebook.sdk.AutoLogAppEventsEnabled" android:value="
    false"/>
<meta-data android:name="com.facebook.sdk.AdvertiserIDCollectionEnabled" android:value
    ="false"/>
uses-permission: android.permission.ACCESS_ADSERVICES_ATTRIBUTION
uses-permission: android.permission.ACCESS_ADSERVICES_AD_ID
uses-permission: android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE
uses-permission: android.permission.ACCESS_ADSERVICES_TOPICS
com.facebook.appevents.gps.pa.PACustomAudienceClient
android.adservices.customaudience.CustomAudienceManager
android.adservices.customaudience.JoinCustomAudienceRequest
joinCustomAudience / setCustomAudience
```

The two disabled Facebook flags are a real mitigation of the default behaviour. The audience-building code and the full permission set are a larger advertising footprint than the flags suggest. A declared permission and a library class show capability and not use. RFI-IRFOS rates the finding LOW, in line with the treatment of advertising permissions elsewhere in the programme. This finding was not mentioned in Roborock's reply and was raised again on 3 September 2026. On 20 November 2026 Roborock stated that the latest version does not contain the Meta Protected Audience-related advertising service permission group. RFI-IRFOS has not checked a later build.

Impact: An advertising audience mechanism is present in an app whose owners use it to run a vacuum cleaner or a lawn mower. Whether any user is placed in an audience is not shown.

Fix: Remove the audience and Privacy Sandbox permissions if they are not used, or say in the policy whether the advertising identifier or audience features are active and on what legal basis.

M1: Exported FCM message 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

com.roborock.smart.msg.FcmMsgService is declared exported true with an intent filter for com.google.firebase.MESSAGING_EVENT. Another app on the device could send a matching intent. Validation inside the service was not examined.

```
<service android:exported="true" android:name="com.roborock.smart.msg.FcmMsgService">
    <intent-filter>
        <action android:name="com.google.firebase.MESSAGING_EVENT"/>
    </intent-filter>
</service>
```

Custom FirebaseMessagingService subclasses are normally not exported. The finding is a component exposure observation. Whether the service validates the intent is UNVERIFIED because dynamic testing was not part of this analysis. On 20 November 2026 Roborock stated that FcmMsgService is a standard component required by Firebase Cloud Messaging and integrated as part of the official SDK. The reply does not say whether the service validates the sender.

Impact: A malicious app on the same phone could try to feed forged notification messages to the Roborock app. Whether it would succeed is not shown.

Fix: Set exported to false and let only the Firebase system component deliver messages, or validate the sender in the service.

M2: Test and staging hostnames in the production build

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 dex contains the literals https://malltest.roborock.com and https://test-cniot.roborock.com next to the production endpoints api-eu, api-us, api-cn, api-ru, euiot, usiot, cn-iot, ruiot and the wood family. The hosts were not contacted.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to LOW because CVSS gives a hostname string with no demonstrated exposure 0.0. The finding is rated LOW because it shows that test infrastructure is referenced from a build shipped to more than 10 million downloads. Whether the hosts are reachable is UNVERIFIED. On 20 November 2026 Roborock stated that the domains not used in the formal version carry no special business logic and have no impact on users. This is not verified by RFI-IRFOS.

```
https://malltest.roborock.com
https://test-cniot.roborock.com
```

Impact: A test host reachable from the internet is an additional surface that is often less hardened than production. Whether these hosts are reachable is not shown.

Fix: Remove test hostnames from production builds and confirm that the test hosts are not reachable from the internet.

M3: Location permissions declared, location absent from the Play Data Safety list of collected data

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 and ACCESS_COARSE_LOCATION, described as optional and used to connect to WiFi, find nearby devices and retrieve details about the current WiFi connection. The Data Safety section read on 23 August 2026 lists device or other IDs, app info and performance, app activity, personal info and photos, and no location.

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 a consumer who compares the permission list with the label sees a mismatch. It may reflect the Google convention that WiFi scanning does not count as collection in the Data Safety sense, and the operator is asked to clarify. On 20 November 2026 Roborock stated that the location information category has been checked and disclosed in the Google Play Data Safety section. RFI-IRFOS has not re-read the label since 23 August 2026.

Impact: A person who reads the Data Safety label before installing sees no location category although the app can request location. The permission is described as optional and tied to WiFi pairing.

Fix: Align the Data Safety declaration with the permissions or explain the convention used.

Impact Analysis

- Households with a robot. A model of the home with rooms and furniture, and a record of cats and dogs, is processed and may be uploaded. The public policy does not mention it (C1).
- People with share access. A family member, a guest or a former partner given share access sees the room structure of the map (C1).
- People in the robot's view. A partner, child, visitor or cleaner can be captured by the live camera and microphone without having agreed (H3).
- EU users. Storage in China is stated in the policy read on 23 August 2026. On 20 November 2026 the operator states storage in Germany for European users, with a transfer mechanism and a representative that RFI-IRFOS has not verified (H1).
- All users. Firebase starts before the consent dialog (C3) and advertising code is present in the package (H4).

The Complete Chain

- 1. A household installs the app and starts Firebase before the consent dialog (C3).
- 2. The robot maps the home. The app holds room names, a map ID and floor type and renders furniture from a labelled library (C1).
- 3. The camera pipeline detects objects. If Pet AI is enabled, pet photos and video are uploaded to a cloud URL behind a separate agreement flag (C1).
- 4. The owner shares the device. A second account reads the room structure (C1).
- 5. The owner opens remote viewing. The robot's camera and microphone capture whoever is present (H3).
- 6. Data is stored in China, Germany and the United States, with limited remote access by group entities abroad (H1).

Each later section refers to one of these links. The harm is that the most intimate model of a private home is held and shared with less explanation in the public policy than the person living there would need.

Home Mapping, Pets & Bystanders

A robot vacuum with a camera and lidar builds a model of a person's life. The rooms and furniture show where people sleep, wash and watch television. A litter tray and a cat bed show a pet. This is not a vulnerability. It is the working feature set of the app, evidenced in the shipped model library and in the Pet AI plugin. What matters is whether the person living there is told, in a document read before first use, that this category of data exists.

Bystanders are the unusual element. Remote viewing and obstacle photos capture whoever is in the room. Art. 13 and Art. 14 require information for people whose data is processed, and a partner or a visitor has no account through which a notice could reach them. The household exemption of Art. 2(2)(c) may cover the account holder's own use. It does not decide the operator's position, because the operator built the feature. Roborock's reply points to a visual indicator and an audio alert on the robot. That is notice to a person in the room and not a legal basis, and it does not answer the DPIA question.

Data Protection: Article by Article

Article	How it is engaged
Art. 5(1)(a)	Transparency. A home map, object and pet recognition and map sharing absent from the public policy read on 23 August 2026 (C1).
Art. 5(1)(c)	Data minimization. Whether the full furniture inventory is needed for cleaning paths, and the capture scope of remote viewing (C1, H3).
Art. 5(2)	Accountability. Burden of showing key restrictions and consent sequencing (C2, C3).
Art. 7(1)	Consent. Firebase provider starts before the consent screen (C3).
Art. 13(1)(c), (e)	Purposes and recipients. Not stated in the public policy for the home model (C1).
Art. 13(1)(f)	Transfer safeguards. Not named in the retrieved policy text (H1).
Art. 27	EU representative. Roborock Germany GmbH named by the operator on 20 November 2026, not verified and not named in the policy text retrieved on 23 August 2026 (H1).
Art. 32(1)(a), (b)	Security of processing. Client credentials (C2), cleartext not blocked (H2), exported service (M1).
Art. 35	DPIA for processing of home layout and for bystander capture. Existence UNVERIFIED (C1, H3).
Art. 44, Art. 46	Transfers to China and other third countries. Mechanism stated by the operator on 20 November 2026 as adequacy decisions and SCC, not verified (H1).

Regulatory & Legal Landscape

The operator is established in China and names Roborock Germany GmbH in Düsseldorf as its GDPR representative. Without an establishment in the Union there is no one-stop-shop lead authority to assume, so this report does not name one. 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: Roborock disabled Crashlytics collection and the Facebook auto-logging and advertiser ID flags, and built a separate agreement flag for pet photos. The same discipline applied to the public policy would close most of C1.

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, and its version and size matched the live Google Play listing.

```
Package       com.roborock.smart
Version       4.72.02 / versionCode 100920
APK           73,948,488 bytes (70.5 MB), SHA-256
    a22037efa3113a6a9f2c05acf19b5a3fd1e87c12a1ac650e4ec9a698f8c8af0a
SDK           minSdkVersion 24, targetSdkVersion 35
Dex           five classes*.dex, about 36,200 unique class-descriptor strings
ICP filing    □□□ICP17032364-4A (res/values/strings.xml)
```

```
https://api-eu.roborock.com   https://euiot.roborock.com   https://wood-eu.roborock.
    com:8010
(and -cn, -us, -ru families)
https://malltest.roborock.com
https://test-cniot.roborock.com
https://rockhome-19f56.firebaseio.com
Project ID           rockhome-19f56
Firebase app ID      1:196751334623:android:576b846efcb16772
Firebase API key     AIzaSyBg_AMeuFMLc7Z9Oy-UXOWXYTthWl2pICM
Google Maps API key  AIzaSyCgKxQATp2aEyz9RoyTLPx0wCgNQsriF08
IoT SDK appkey       rr
IoT SDK appsecret    qWKYcdQWrbm9hPqe
Facebook App ID      554874373514387
Facebook client token 07c7262b04c7cece2a4ecc43e525b324
Policy               https://global.roborock.com/pages/privacy-policy
```

```
dpo@roborock.com          privacy contact named in the policy
privacy@roborock-eu.com    EEA privacy contact named in the policy
privacy@roborock.com       sender of the replies of 2026-08-31 and 2026-11-20
Roborock Germany GmbH      Peter-Müller-Strasse 16/16a, 40468 Düsseldorf, GDPR
    representative named on 2026-11-20
support@roborock-eu.com    EU-routed support
```

Disclosure Timeline & Outcome

Date	Event
2026-08-23	Analysis of version 4.72.02. Notice REF ROBOROCK-2026-R1 sent to dpo@roborock.com and privacy@roborock-eu.com, copied to the Datenschutzbehörde and the EDPS. Seven findings itemised and three written questions.
2026-08-31	Reply from privacy@roborock.com. It states that the features are disclosed in the device privacy policies shown after network configuration, that the remote-viewing stream is not stored and is relayed encrypted only under certain network conditions, that the robot shows a visual indicator and plays an audio alert, that the App Privacy Policy names an EU representative in Germany and a transfer mechanism, that the Firebase and Maps keys and the Facebook App ID configuration follow vendor guidance, and that the flagged issues are false positives of an automated scanning tool. It adds that other issues are being studied.
2026-09-03	Follow-up from RFI-IRFOS to dpo@roborock.com, privacy@roborock-eu.com and privacy@roborock.com. It lists findings 1, 3 and 7 as unanswered, accepts the Firebase point, describes the analysis as manual root level code analysis, and restates three questions. Written answer requested by 17 September 2026.
2026-11-15	Reminder from s.kepp@rfi-irfos.com to dpo@roborock.com, privacy@roborock-eu.com and privacy@roborock.com, 6 days before publication. It restates the findings and the three questions and names 21 November 2026 as the publication date.
2026-11-20	Reply from privacy@roborock.com. It answers the three questions: device privacy policies with one linked example, no data controller role for the remote-viewing stream, storage in Germany, SCC and adequacy for transfers, Roborock Germany GmbH as GDPR representative. For the latest version, version number not named, it states that the appsecret is removed from the client code, that Firebase starts after the consent screen, that only HTTPS is permitted and that the Meta advertising permission group is absent. It calls M1 a standard component and M2 without impact and says Data Safety covers audio, video and location. Not verified by RFI-IRFOS.
2026-11-21	Publication of this report, 90 days after delivery of the notice.

The operator received the same embargo date in every message. No request to extend it was made and none was granted. The second reply arrived on 20 November 2026, 78 days after the follow-up of 3 September 2026 and one day before publication.

What Roborock Got Right

- allowBackup is false, so app data is excluded from Android automatic cloud backup.
- Firebase Crashlytics collection is disabled by manifest flag.
- The Facebook SDK flags AutoLogAppEventsEnabled and AdvertiserIDCollectionEnabled are set to false.
- BLUETOOTH_SCAN is declared with usesPermissionFlags neverForLocation, which separates Bluetooth scanning from location inference.
- A separately worded agreement flag exists for pet photo uploads, which shows that the category was recognised as needing its own gate.
- Region-partitioned backend endpoint families allow data residency controls. Whether EU accounts stay on EU endpoints is UNVERIFIED.
- The app targets API 35 and is actively maintained.
- Roborock answered within eight days, engaged with the findings in writing and says other issues are being studied.
- On 20 November 2026 Roborock replied point by point and states for the latest version that it removed the IoT SDK appsecret from the client code, moved Firebase initialisation behind the consent screen, limited traffic to HTTPS and dropped the Meta advertising permission group. These are operator statements that RFI-IRFOS has not verified.

Residual Risk & Recommendations

All ten findings keep their severity for version 4.72.02. Roborock answered the three questions on 20 November 2026 and states fixes in the latest version for C2, C3, H2 and H4, which RFI-IRFOS has not checked. It treats M1 and M2 as standard or harmless and points to one device privacy policy for C1, which was not read. Versions after 4.72.02 are not covered. The device privacy policies, the payload of any upload and the behaviour of the appsecret were not examined.

- Name the home map, object and pet recognition and device sharing in the public privacy policy that precedes purchase, and state where recognition runs and how long data is kept.
- Publish the DPIA conclusions for the home model and for remote viewing, and state the consent or notice basis for bystanders.
- Name the Art. 46 mechanism per storage location and the Art. 27 representative with address.
- Start Firebase after the consent state is known, and remove the Privacy Sandbox permissions if they are unused.
- Block cleartext traffic in the base network configuration, and remove test hostnames from production builds.
- Show the restriction of the Maps key, state what the IoT appsecret authorizes, and protect FcmMsgService.

- Name the app version in which each fix shipped, so that it can be checked against the package.

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 policy and Google Play listing. No Roborock 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 ROBOROCK-2026-R1.