



Security & Privacy Disclosure, Final Report

Smart Life (com.tuya.smartlife)

A Chinese-operated smart-home app requests 27 Android Health Connect permissions including blood pressure and heart rate, integrates a full in-home camera/microphone/door-lock surveillance stack with geofencing, routes server traffic through an encrypted, non-inspectable region bundle secured by a hardcoded app-encryption secret, and embeds a remote mini-program execution engine, unresolved through nine messages over 68 days and a 19-day-overdue embargo with zero reply of any kind

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28
SEPTEMBER 2026, NINE FINDINGS REMAIN UNADDRESSED**

Target	Hangzhou Thing Information Technology Co., Ltd. (Tuya Inc., Hangzhou, PRC; NYSE: TUYA)
Package	com.tuya.smartlife (Smart Life – Smart Living), consumer twin of com.tuya.smart
Platform Audited	Android, static analysis of the production APK (base + arm64 splits, apktool/dex-strings/NSC/SDK-fingerprint)
Initial Disclosure (R1)	2026-06-30 (REF SMARTLIFE-2026-R1-001)
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	9 (3 Critical, 4 High, 2 Medium)
Correspondence	9 messages sent by RFI-IRFOS to privacy@tuya.com over 68 days; zero reply of any kind, zero bounce, zero acknowledgment ever received
Authorities CC'd	Austrian Datenschutzbehörde (DSB) · European Data Protection Supervisor (EDPS), BCC'd or CC'd on correspondence

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	Subject & Operator Context	5
3	Engagement Summary	6
4	Findings	6
4.1	C1: 27 Android Health Connect permissions, including blood pressure, heart rate, and SpO2, on a smart-home app	6
4.2	C2: Whole-home surveillance and occupancy/presence inference: camera, microphone, door lock, geofence, location	7
4.3	C3: PRC operator plus Alibaba/Tencent/ByteDance infrastructure, with encrypted, non-inspectable region routing	8
4.4	H1: Hardcoded secrets: Tuya app-encryption secret, AMap key, two Google/Firebase keys, and a Firebase RTDB URL	9
4.5	H2: Insecure transport: cleartext traffic permitted globally in production	9
4.6	H3: Pre-consent SDK auto-init: Firebase, AdMob, MLKit, and Tuya's own bootstrap initialize before any consent gate	10
4.7	H4: Embedded mini-program engine: remote code and dynamic content execution with native bridge access	10
4.8	M1: No EU Art. 27 representative or DPO evidenced in binary; Chinese OEM push SDK app-IDs	11
4.9	M2: Calendar read/write plus overlay, battery-exemption, and high-rate sensor access with no disclosed purpose	11
5	Impact Analysis	12
6	The Complete Chain: Nine Messages, Zero Replies, Zero Acknowledgments	12
7	Data Protection – Article by Article	13
8	Regulatory & Legal Landscape	13
9	Indicators of Compromise	14
10	Disclosure Timeline & Outcome	14
11	Residual Risk & Recommendations	15

Executive Summary

Smart Life (com.tuya.smartlife, v7.8.6) is the consumer smart-home companion app from Tuya Inc. (Hangzhou, PRC), the direct twin of com.tuya.smart, which RFI-IRFOS previously rated CRITICAL for the same structural issues. A root-level static analysis of the production Android binary found nine findings, three CRITICAL, four HIGH, and two MEDIUM.

The app requests 27 Android Health Connect permissions, including READ access to blood pressure, heart rate, and blood-oxygen saturation, and WRITE access to blood pressure, body temperature, basal metabolic rate, and body fat, and ships a dedicated health-AI data module ('com.thingclips.smart.health.ai.data'), on an app whose primary purpose is plugs, bulbs, cameras, and door locks (C1). The app is also a whole-home surveillance and presence-inference platform: it holds fine, coarse, and background location, a full geofencing engine, Bluetooth and Wi-Fi scanning, and the complete IPC camera/NVR stack alongside door locks with NFC keys, motion detection, and a home-security/alarm module, plus RECORD_AUDIO and FOREGROUND_SERVICE_MICROPHONE for two-way audio; geofence transitions combined with device state produce a continuously updated household occupancy signal (C2). The operating entity is Hangzhou Thing Information Technology Co., Ltd. (Tuya's PRC entity), and the binary integrates AMap (Alibaba), Alibaba Cloud OSS, Tencent WeChat, Alibaba fastjson, and ByteDance native instrumentation; server endpoints are not present in plaintext anywhere in the binary but are carried in an encrypted region-routing bundle decrypted at runtime with a hardcoded app-encryption secret, making the actual destination datacenter for a given EU user non-inspectable from the shipped artifact (C3).

Four further HIGH findings compound the pattern: the Tuya app-encryption secret (the key that unlocks the region/pin bundle in C3), an AMap key, two Google/Firebase keys, and a Firebase Realtime Database URL are all hardcoded verbatim in 'strings.xml' (H1); the production network security configuration permits cleartext traffic globally (H2); roughly a dozen SDKs including Firebase, AdMob, MLKit, and Tuya's own bootstrap auto-initialize via ContentProviders before any consent gate, while the app holds the advertising-ID and Privacy Sandbox permission set (H3); and the app embeds a full WeChat-style mini-program engine capable of loading and executing remotely delivered code with native bridge access to device capabilities, meaning the processing actually performed is not fully determined by the shipped binary (H4). Two MEDIUM findings close the picture: no EU Art. 27 representative or DPO evidenced in the binary, alongside configuration for the Chinese OEM push ecosystems (Xiaomi, OPPO, Meizu, Huawei, Honor, Vivo) (M1), and calendar read/write plus overlay, battery-optimization exemption, and high-rate sensor access with no disclosed purpose (M2).

RFI-IRFOS disclosed these findings on 30 June 2026 to privacy@tuya.com, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor BCC'd, stating an embargo date of 28 September 2026. Over the following 68 days RFI-IRFOS sent eight further messages (6 July, 17 July, 23 July, 31 July, 9 August, 21 August, 28 August, 6 September 2026), each restating the findings and the three direct questions, with the DSB intermittently moved into CC. Across all nine messages, RFI-IRFOS received zero reply of any kind: not a bounce, not an automated acknowledgment, not a single word.

ID	Severity	Title
C1	CRITICAL	27 Android Health Connect permissions, including blood pressure, heart rate, and SpO2, on a smart-home app

ID	Severity	Title
C2	CRITICAL	Whole-home surveillance and occupancy/presence inference: camera, microphone, door lock, geofence, location
C3	CRITICAL	PRC operator plus Alibaba/Tencent/ByteDance infrastructure, with encrypted, non-inspectable region routing
H1	HIGH	Hardcoded secrets: Tuya app-encryption secret, AMap key, two Google/Firebase keys, and a Firebase RTDB URL
H2	HIGH	Insecure transport: cleartext traffic permitted globally in production
H3	HIGH	Pre-consent SDK auto-init: Firebase, AdMob, MLKit, and Tuya's own bootstrap initialize before any consent gate
H4	HIGH	Embedded mini-program engine: remote code and dynamic content execution with native bridge access
M1	MEDIUM	No EU Art. 27 representative or DPO evidenced in binary; Chinese OEM push SDK app-IDs
M2	MEDIUM	Calendar read/write plus overlay, battery-exemption, and high-rate sensor access with no disclosed purpose

Subject & Operator Context

Smart Life is the consumer-facing twin of Tuya Smart (com.tuya.smart), both built on Tuya Inc.'s "Thing" SDK. The operating entity named verbatim in the app's own Thing Smart Platform agreement string is Hangzhou Thing Information Technology Co., Ltd., the PRC operating entity of Tuya Inc. (Hangzhou, China; NYSE: TUYA). RFI-IRFOS had already rated the sibling app com.tuya.smart **CRITICAL** for structurally identical findings (27 Health Connect permissions, a hardcoded IoT-platform key, and PRC National Intelligence Law exposure) under a separate REF.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to privacy@tuya.com, BCC the Austrian Datenschutzbehörde and the European Data Protection Supervisor, stating an embargo date of 28 September 2026 under REF SMARTLIFE-2026-R1-001. RFI-IRFOS followed up on 6 July, 17 July, 23 July, 31 July, 9 August, 21 August, 28 August, and 6 September 2026, with the DSB intermittently moved into CC. Nine messages were sent in total over 68 days. No reply of any kind, automated or human, and no delivery failure, was ever received.

Findings

C1: 27 Android Health Connect permissions, including blood pressure, heart rate, and SpO2, on a smart-home app

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.3) — special-category health data permissions on a plugs-and-bulbs app, wired to a dedicated health-AI module

```
android.permission.health.READ_BLOOD_PRESSURE    android.permission.health.
WRITE_BLOOD_PRESSURE
android.permission.health.READ_HEART_RATE    android.permission.health.WRITE_HEART_RATE
android.permission.health.READ_OXYGEN_SATURATION    android.permission.health.
WRITE_OXYGEN_SATURATION
android.permission.health.WRITE_BODY_TEMPERATURE    android.permission.health.
WRITE_BASAL_METABOLIC_RATE
(27 distinct Health Connect permissions total)

Lcom/thingclips/smart/health/ai/data/api/bean/
Lcom/thingclips/smart/health/ai/data/manager/
```

Impact: The app declares 27 Android Health Connect permissions, including READ access to blood pressure, heart rate, and blood-oxygen saturation, and WRITE access to blood pressure, body temperature, basal metabolic rate, body fat, bone mass, and body-water mass, and ships a dedicated health data module ('com.thingclips.smart.health.ai.data') wired to a health-AI pipeline. Blood pressure, heart rate, SpO2, body composition, and sleep are special-category data concerning health under Art. 9(1), requiring an Art. 9(2) basis and a mandatory Art. 35 DPIA for large-scale special-category processing, a scope difficult to reconcile with Art. 5(1)(c) minimisation for an app whose stated purpose is smart-home device control.

C2: Whole-home surveillance and occupancy/presence inference: camera, microphone, door lock, geofence, location

CRITICAL (CVSS v4.0 AV:P/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.0) — full in-home camera/NVR, two-way audio, and door-lock control combined with background-location geofencing for continuous occupancy inference

```
android.permission.ACCESS_BACKGROUND_LOCATION  android.permission.CAMERA  android.
permission.RECORD_AUDIO
android.permission.FOREGROUND_SERVICE_MICROPHONE  android.permission.NFC
Lcom/thingclips/smart/camera/ipccamerasdk/  Lcom/thingclips/smart/homearmed/...
com.thingclips.smart.doorlock.nfc.DoorlockPhoneKeyActivity
GeofenceManager  GeofencingModeActivity  GeofenceTrait (100+ refs)
lib/arm64-v8a/libThingCameraSDK.so  libThingP2PSDK.so  libThingMotionDetectSDK.so
```

Impact: The app integrates the full IPC camera/NVR stack, two-way audio (RECORD_AUDIO plus FOREGROUND_SERVICE_MICROPHONE and native audio-engine libraries), motion detection, a home-security/alarm module, NFC door-lock control, and a geofencing engine (100+ references), while holding fine, coarse, and background location plus Bluetooth and Wi-Fi scanning. Continuous in-home video and audio capture and door-lock state are highly sensitive and can engage Art. 9 for identifiable persons; geofence transitions combined with device on/off state constitute regular, systematic monitoring under Art. 35(3)(c) that produces a continuously updated household presence/occupancy signal, engaging Art. 5(1)(c) minimisation and Art. 25 data protection by design.

C3: PRC operator plus Alibaba/Tencent/ByteDance infrastructure, with encrypted, non-inspectable region routing

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 7.5) — RFI-IRFOS blast-radius escalation: raised to CRITICAL because the encrypted routing bundle makes it structurally impossible for an EU data subject or regulator to determine which third country receives their data, not because the encryption itself was broken

```
Thing Smart Platform agreement: "...provided by Hangzhou Thing Information Technology Co., Ltd..."
<data android:host="smartlife.app.tuya.com" .../>
amapKey: [REDACTED IN PUBLIC REPORT -- disclosed privately to Tuya in R1] (AMap = Gaode/Alibaba, China)
Lcom/tencent/mm/opensdk/... (Tencent WeChat SDK) Lcom/alibaba/fastjson/... (334+ refs)
Lcom/bytedance/shadowhook/... (ByteDance native hook)

assets/thing_domains_v1/regions (encrypted region->endpoint map)
assets/thing_domains_v1/pins (encrypted certificate-pin set)
appEncryptSecretProdV2: [REDACTED IN PUBLIC REPORT -- disclosed privately to Tuya in R1]
```

Impact: The operating entity named in the binary's own Thing Smart Platform agreement string is Hangzhou Thing Information Technology Co., Ltd. The binary integrates AMap (Gaode/Alibaba, China) as its maps provider, Alibaba Cloud OSS, the Tencent WeChat SDK, Alibaba's fastjson JSON layer, and ByteDance native instrumentation. Server endpoints are not present in plaintext anywhere in dex, resources, or native libraries; they are carried in an encrypted region-routing bundle ('assets/thing_domains_v1/regions' and 'pins') decrypted at runtime with a hardcoded app-encryption secret, alongside a custom Tuya CA. A PRC-headquartered operator with Alibaba/Tencent/ByteDance components engages GDPR Chapter V and the PRC National Intelligence Law (Art. 7); the encrypted, non-inspectable region routing is itself an accountability and transparency problem, since a data subject cannot determine from the app which third country, if any, receives their data.

H1: Hardcoded secrets: Tuya app-encryption secret, AMap key, two Google/Firebase keys, and a Firebase RTDB URL

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.5)
— the recovered app-encryption secret is also the key that protects C3's region/pin bundle

```
appEncryptSecretProdV2: [REDACTED IN PUBLIC REPORT -- disclosed privately to Tuya in R1]
appEncryptSecretCvProdV2: [REDACTED IN PUBLIC REPORT -- disclosed privately to Tuya in R1]
amapKey: [REDACTED IN PUBLIC REPORT -- disclosed privately to Tuya in R1]
google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Tuya in R1]
google_maps_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Tuya in R1]
firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately to Tuya in R1]
]
project_id: smartlife-3926a
```

Impact: The Tuya app-encryption secrets (the key that decrypts the C3 region/pin bundle), the AMap maps key, two Google/Firebase API keys, the Firebase project identifier, and a Firebase Realtime Database URL are all extractable verbatim from 'res/values/strings.xml'. The app-encryption secret lowers the bar to decrypting Tuya's own region/pin protection; an unrestricted Google/Firebase key enables quota/billing exhaustion, and any misconfigured Firebase rule becomes a data-exposure path. Under Art. 32 the burden is on the operator to prove each key is scoped.

H2: Insecure transport: cleartext traffic permitted globally in production

HIGH (CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3)
— production base-config permits cleartext to any host not otherwise overridden

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

Impact: The production network security configuration's 'base-config' permits cleartext (HTTP) traffic globally for every domain not otherwise overridden. Tuya does apply app-level pinning for its own endpoints via the encrypted 'thing_domains_v1/pins' bundle, but the platform-level cleartext bar remains wide open for any other host the app or its mini-programs contact, substantially lowering the bar for interception on a modern target SDK.

H3: Pre-consent SDK auto-init: Firebase, AdMob, MLKit, and Tuya's own bootstrap initialize before any consent gate

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.5)
 — advertising identifiers and Privacy Sandbox permissions held while providers initialize before consent

```
<provider android:name="com.google.firebase.provider.FirebaseInitProvider" .../>
<provider android:name="com.google.android.gms.ads.MobileAdsInitProvider" android:
  initOrder="100"/>
<provider android:name="com.google.mlkit.common.internal.MLKitInitProvider"/>
<provider android:name="com.thingslips.smart.optimus.sdk.ThingOptimusProvider"/>

com.google.android.gms.permission.AD_ID
android.permission.ACCESS_AD_SERVICES_AD_ID / _ATTRIBUTION / _TOPICS
```

Impact: Firebase, AdMob (initOrder 100), MLKit, and Tuya's own Optimus SDK bootstrap all initialize via ContentProvider at application process start, before any consent UI can appear. The app holds the AD_ID permission plus the full ACCESS_AD_SERVICES Privacy Sandbox set and integrates the AdMob ad and mediation stack. A Google UMP/IAB-TCF consent surface is present but, on the static evidence, gates AdMob only, not the Firebase/MLKit/Optimus providers that have already initialized by the time it can act.

H4: Embedded mini-program engine: remote code and dynamic content execution with native bridge access

HIGH (CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 5.9)
 — a WeChat-style mini-program engine can load and execute server-delivered logic with bridge access to device capabilities

```
Lcom/gzl/smart/gzlminiapp/... (3,872 class refs) "MiniProgram" 216 refs
assets/mini_app_js/ assets/mini_widget/ assets/thing_uni_plugins/ assets/kit_js/
WebViewActivity / WebInterceptActivity / jsbridge.* (com.thingslips.smart.jsbridge)
```

Impact: The app ships a full WeChat-style mini-program engine ('gzlminiapp', 3,872 class references) plus a JS-bridge and bundled JS runtimes, capable of loading and executing remotely delivered mini-apps or Uni-plugins inside the app with native bridge access to device capabilities. A dynamic code/content-loading surface of this kind means the processing actually performed by the app is not fully determined by the shipped binary and can change server-side without re-review, undermining the transparency that Art. 5(1)(a) and Art. 25/32 presume is achievable from the published artifact.

M1: No EU Art. 27 representative or DPO evidenced in binary; Chinese OEM push SDK app-IDs

MEDIUM (CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 3.1) — accountability gap compounding the PRC infrastructure picture in C3

```
mi_app_id: 2882303761517474496 (Xiaomi push)   oppo_app_id: 3585286 (OPPO push)
meizu_app_id: 112715 (Meizu push)   huawei_app_id: 10539770 (Huawei push)
vivo_app_key: d0a642e7-a564-4f04-9e2d-afab86d0f8f4
```

Impact: The app ships configuration for the Chinese OEM push ecosystems (Xiaomi, OPPO, Meizu, Huawei, Honor, Vivo) alongside FCM, corroborating the PRC infrastructure picture in C3. The app's privacy policy is served dynamically with no static URL extractable from the binary, so no Art. 27 EU representative and no DPO could be confirmed from the binary. Locales include de/de-DE, establishing EU targeting. A controller outside the EU offering services to EU data subjects must designate a written Art. 27 representative and, given the large-scale special-category processing in C1 and systematic monitoring in C2, likely a DPO under Art. 37.

M2: Calendar read/write plus overlay, battery-exemption, and high-rate sensor access with no disclosed purpose

MEDIUM (CVSS v4.0 AV:P/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 4.3) — permissions beyond the surveillance/health sets already documented in C1/C2

```
android.permission.READ_CALENDAR   android.permission.WRITE_CALENDAR
android.permission.SYSTEM_ALERT_WINDOW   android.permission.
    REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
android.permission.HIGH_SAMPLING_RATE_SENSORS
```

Impact: Beyond the surveillance and health permission sets in C1 and C2, the app holds calendar read and write (used for check-in reminders), screen-overlay (SYSTEM_ALERT_WINDOW), battery-optimization exemption, legacy external-storage, high-sampling-rate sensors, and the Play install-referrer binding. Calendar access and high-rate sensor sampling on a smart-home app press on Art. 5(1)(c) minimisation, and the battery-exemption plus overlay support always-on background behaviour relevant to the presence-inference concern in C2.

Impact Analysis

C1 and C2 establish that Smart Life collects special-category health data and whole-home surveillance signals, including camera, audio, and door-lock state, that together with geofencing produce a continuous household presence profile. C3 establishes that the operator is a PRC entity routing that data through an encrypted, non-inspectable region bundle secured by a key extractable from the same binary (H1). H2 through H4 are transport and execution-surface weaknesses layered on top: global cleartext permission, pre-consent SDK initialization, and a remote code-execution engine that means the binary alone cannot fully describe what the app does at runtime. M1 and M2 close the picture with an accountability gap and a residual over-collection of permissions.

What ties all nine findings together procedurally is the correspondence record: nine messages, sent to one named, functioning address over 68 days, drew zero reply of any kind, not an automated acknowledgment, not a bounce, not a single word.

The Complete Chain: Nine Messages, Zero Replies, Zero Acknowledgments

Step 1 – Disclosure sent: RFI-IRFOS sends the full findings report on 30 June 2026 to privacy@tuya.com, BCC the Austrian Datenschutzbehörde and the EDPS, stating an embargo date of 28 September 2026.

Step 2 through 8 – Seven follow-ups, identical outcome: RFI-IRFOS sends further messages on 6 July, 17 July, 23 July, 31 July, 9 August, 21 August, and 28 August 2026, each restating the three direct questions and the days elapsed. No reply, no bounce, no acknowledgment is received at any point.

Step 9 – Final follow-up: On 6 September 2026, RFI-IRFOS sends a ninth and final message, 68 days after the original disclosure. No further correspondence follows.

Step 10 – Embargo reached and passed: The embargo, stated once on 30 June 2026 and never revised, passes on 28 September 2026 with all nine findings unaddressed.

Step 11 – Publication: This report publishes 19 days after the embargo date. Across 68 days and nine messages sent to a single functioning address, the correspondence record contains zero replies of any kind.

Data Protection – Article by Article

Art. 9, 35, 5(1)(c), 6 GDPR – Special-category health data, DPIA, data minimisation: C1's 27 Health Connect permissions on a smart-home app.

Art. 9, 6, 5(1)(b)/(c), 25, 35(3)(c), 32 GDPR – Special-category data, systematic monitoring, data protection by design: C2's whole-home surveillance and occupancy-inference stack.

Art. 44, 46, 13(1)(f), 5(1)(a)/(2), 35 GDPR – Third-country transfer, transparency, accountability: C3's PRC operator and encrypted, non-inspectable region routing.

Art. 32 GDPR – Security of processing: H1's hardcoded app-encryption secret and API keys.

Art. 32, 25 GDPR – Security and data protection by design: H2's globally cleartext-permitting production transport configuration.

Art. 6(1), 7(1), 5(1)(a)/(2) GDPR; ePrivacy Art. 5(3) – Lawfulness and consent preceding processing: H3's pre-consent SDK auto-initialization.

Art. 25, 32, 5(1)(a) GDPR – Data protection by design and transparency: H4's remote mini-program execution engine.

Art. 27, 37, 13(1)(a)/(b) GDPR – EU representative, DPO, transparency: M1's absence of any named EU representative.

Art. 5(1)(b)/(c), 6 GDPR – Purpose limitation and data minimisation: M2's residual permission over-collection.

Regulatory & Legal Landscape

Hangzhou Thing Information Technology Co., Ltd. (Tuya Inc.) has no EU main establishment or Art. 27 representative evidenced in the binary, so no one-stop-shop mechanism is established from the artifact. RFI-IRFOS's lead reporting authority for this case is the Austrian Datenschutzbehörde (DSB), informed in BCC on the initial disclosure and intermittently in CC on follow-ups, alongside the European Data Protection Supervisor, under GDPR Art. 83(2)(b).

Fine exposure under GDPR: Art. 83(5) applies to the Art. 9/35 special-category issues in C1 and C2 and the Art. 44/46 transfer issue in C3, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 32/25/6/7 issues in H1 through H4 and the Art. 27/37/5(1)(c) issues in M1 and M2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. An operator of a NYSE-listed company's consumer app that received nine written disclosures over 68 days and did not reply even once is itself a fact a regulator is likely to weigh alongside the nine technical findings.

Indicators of Compromise

The following identifiers, SDK packages, and manifest declarations were extracted from the production APK via static analysis only. No Tuya, Alibaba, Tencent, or ByteDance servers, accounts, or infrastructure were probed.

```
C1 -- 27 Health Connect permissions; com.thingclips.smart.health.ai.data module

C2 -- ACCESS_BACKGROUND_LOCATION, CAMERA, RECORD_AUDIO; GeofenceManager;
    DoorlockPhoneKeyActivity

C3 -- smartlife.app.tuya.com; assets/thing_domains_v1/{regions,pins}; AMap/Alibaba OSS
    /Tencent WeChat SDKs

H1 -- appEncryptSecretProdV2, amapKey, google_api_key, firebase_database_url in
    strings.xml (redacted above)

H2 -- network_security_config.xml: cleartextTrafficPermitted="true" in base-config

H3 -- FirebaseInitProvider, MobileAdsInitProvider (initOrder 100),
    ThingOptimusProvider

H4 -- Lcom/gzl/smart/gzlminiapp (3,872 refs); assets/mini_app_js/, assets/
    thing_uni_plugins/

M1 -- mi_app_id, oppo_app_id, huawei_app_id (Chinese OEM push configuration)

M2 -- READ_CALENDAR, WRITE_CALENDAR, SYSTEM_ALERT_WINDOW, HIGH_SAMPLING_RATE_SENSORS
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to privacy@tuya.com, BCC Austrian DSB and EDPS. Embargo stated as 2026-09-28. REF SMARTLIFE-2026-R1-001.

2026-07-06, 2026-07-17, 2026-07-23, 2026-07-31, 2026-08-09, 2026-08-21, 2026-08-28
Seven follow-up messages, each restating the nine findings and the three direct questions. No reply, no bounce, no acknowledgment at any point.

2026-09-06 Ninth and final message sent, 68 days since the original disclosure. No further correspondence follows.

2026-09-28 Embargo date reached, as stated once on 2026-06-30 and never revised. Correspondence record: nine RFI-IRFOS messages, zero replies.

2026-10-17 This report published, 19 days after the embargo date. All nine findings confirmed unaddressed on the basis of the correspondence record.

Residual Risk & Recommendations

C1 – Immediate: document the Art. 9(2) basis and Art. 35 DPIA for the Health Connect permission scope, or remove permissions with no demonstrated smart-home purpose.

C2 – Immediate: document the Art. 6 basis for background-location geofencing and the Art. 35(3)(c) DPIA for occupancy inference.

C3 – Immediate: disclose the destination datacenter logic in the privacy policy and document an Art. 46 transfer safeguard and transfer-impact assessment covering the management/O TA/support plane.

H1 – Near-term: rotate and restrict all hardcoded keys and secrets, including the app-encryption secret.

H2 – Near-term: disable global cleartext in the production network security configuration.

H3 – Near-term: gate all SDK initialization, not only AdMob, behind the existing consent management platform.

H4 – Near-term: document the review and security process applied to mini-programs loaded at runtime.

M1 – Near-term: designate a written Art. 27 EU representative and a DPO under Art. 37.

M2 – Near-term: remove or justify calendar, overlay, and high-rate sensor permissions.

Across all findings: establish a monitored intake path for security and data-protection disclosures sent to privacy@tuya.com that produces at minimum an acknowledgment, which nine messages over 68 days failed to produce.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of the published application using publicly available tooling. No Tuya, Alibaba, Tencent, or ByteDance servers, accounts, or infrastructure were probed. Technical evidence is archived under chain of custody and will be provided to regulatory authorities on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF SMARTLIFE-2026-R1-001.