



---

# Security & Privacy Disclosure, Final Report

Linky / iChat, AI-companion and live-social app  
(com.aigc.ushow.ichat)

An AI-companion app offering sexual/romantic roleplay behind a self-declared-birthday age gate ships a Chinese biometric face-liveness stack and saturates its binary with Chinese-origin advertising, analytics, cloud-storage and voice-transcription SDKs that its own privacy policy never once names or discloses as Chinese, and eight follow-ups over 74 days drew eight identical automated support-desk acknowledgments, never once a human reply engaging any finding

**PUBLIC DISCLOSURE, 17 OCTOBER 2026 — EMBARGO REACHED 28  
SEPTEMBER 2026, EIGHT IDENTICAL AUTOMATED REPLIES RECEIVED, ZERO  
HUMAN ENGAGEMENT, THREE QUESTIONS NEVER ANSWERED**

---

|                                  |                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target</b>                    | Skywork AI Pte. Ltd. (Singapore) — declared controller per the published privacy policy; operational backend and native engine run by USHOW Media (StarMaker), relationship between the two left unclarified by the controller                                                                                            |
| <b>Package</b>                   | com.aigc.ushow.ichat v3.30.0 (versionCode 62542059)                                                                                                                                                                                                                                                                       |
| <b>Platform Audited</b>          | Android, static analysis of the production APK (base + arm64 split)                                                                                                                                                                                                                                                       |
| <b>Initial Disclosure (R1)</b>   | 2026-06-30, to support@linke.ai, BCC (later visible CC) Austrian Datenschutzbehoerde and EDPS                                                                                                                                                                                                                             |
| <b>Disclosure / Embargo Date</b> | 2026-09-28                                                                                                                                                                                                                                                                                                                |
| <b>Report Published</b>          | 2026-10-17                                                                                                                                                                                                                                                                                                                |
| <b>Overall Severity</b>          | CRITICAL                                                                                                                                                                                                                                                                                                                  |
| <b>Findings</b>                  | 9 (2 Critical, 6 High, 1 Medium)                                                                                                                                                                                                                                                                                          |
| <b>Correspondence</b>            | 8 messages sent by RFI-IRFOS over 74 days (2026-06-30 to 2026-09-12), 8 automated support-desk acknowledgments received, one after each message, all textually identical, none engaging a single finding, legal citation, or any of the three questions asked — not silence, but no human reply of substance at any point |
| <b>Authorities Notified</b>      | Austrian Datenschutzbehoerde (dsb@dsb.gv.at) · European Data Protection Supervisor (EDPS, edps@edps.europa.eu)                                                                                                                                                                                                            |

---

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

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

## Contents

|           |                                                                                                                                                                         |           |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1</b>  | <b>Executive Summary</b>                                                                                                                                                | <b>4</b>  |
| <b>2</b>  | <b>Subject &amp; Operator Context</b>                                                                                                                                   | <b>5</b>  |
| <b>3</b>  | <b>Engagement Summary</b>                                                                                                                                               | <b>6</b>  |
| <b>4</b>  | <b>Findings</b>                                                                                                                                                         | <b>6</b>  |
| 4.1       | C1: Binary saturated with Chinese-origin SDKs and cloud endpoints (ByteDance, Mintegral, Tencent, Alibaba, ZEGO); China never disclosed in the privacy policy . . . . . | 6         |
| 4.2       | C2: Ant Group/Alibaba 'Toyger'-class biometric face-liveness stack compiled in; vendor and PRC transfer undisclosed . . . . .                                           | 7         |
| 4.3       | C3: Sexual/romantic AI companion content ('Passion Mode') behind a self-declared-birthday age gate . . . . .                                                            | 8         |
| 4.4       | H1: Pre-consent SDK auto-initialization; no consent-management platform; Facebook auto-collects the advertising identifier . . . . .                                    | 9         |
| 4.5       | H2: Voice capture routed to Tencent Cloud real-time speech recognition on a platform offering intimate conversation and live voice rooms . . . . .                      | 9         |
| 4.6       | H3: Cleartext traffic permitted globally; no certificate pinning on any domain including the app's own APIs; backup allowed . . . . .                                   | 10        |
| 4.7       | H4: Firebase/Google API key hardcoded in the distributed binary (project linkme-49e8a) . . . . .                                                                        | 10        |
| 4.8       | H5: Chinese OAID device-identifier harvesting stack feeding two attribution SDKs and roughly ten ad networks simultaneously . . . . .                                   | 11        |
| 4.9       | M1: Broad permission, overlay, and accounts surface, plus an ad-SDK in-app APK install funnel . . . . .                                                                 | 11        |
| <b>5</b>  | <b>Impact Analysis</b>                                                                                                                                                  | <b>12</b> |
| <b>6</b>  | <b>The Complete Chain: Eight Messages, 74 Days, Eight Identical Automated Replies, Zero Human Engagement</b>                                                            | <b>12</b> |
| <b>7</b>  | <b>Data Protection – Article by Article</b>                                                                                                                             | <b>13</b> |
| <b>8</b>  | <b>Regulatory &amp; Legal Landscape</b>                                                                                                                                 | <b>13</b> |
| <b>9</b>  | <b>Indicators of Compromise</b>                                                                                                                                         | <b>14</b> |
| <b>10</b> | <b>Disclosure Timeline &amp; Outcome</b>                                                                                                                                | <b>14</b> |
| <b>11</b> | <b>Residual Risk &amp; Recommendations</b>                                                                                                                              | <b>15</b> |

## Executive Summary

Linky (consumer domain linke.ai, package com.aigc.ushow.ichat) is an AI-companion and live-social app whose core offering includes sexual/romantic AI roleplay ('Passion Mode', an NSFW switch) alongside live audio/video rooms. Its published privacy policy names Skywork AI Pte. Ltd. (Singapore) as controller; the production backend and native engine run on USHOW Media's StarMaker codebase. Skywork AI is publicly associated with the Chinese AI group Kunlun Tech. No EU Art. 27 representative and no DPO are named anywhere in the binary or the privacy policy.

Static analysis of the production APK found the binary saturated with Chinese-origin SDKs and native engines, ByteDance Pangle, Mintegral/Mobvista, Tencent Beacon/COS/TRTC/LiteAV/Cloud-ASR, Alibaba Cloud OSS and CloudAuth face-verification, and ZEGO's real-time engine, hard-coding Chinese cloud hostnames including Hong Kong and Shanghai regions, while the privacy policy does not mention China once. A full Ant Group/Alibaba 'Toyger'-class biometric face-liveness stack is compiled in, with the privacy policy disclosing only a generic 'one-time facial image through a third-party service' with no vendor named and no transfer disclosed. The app's sexual/romantic content sits behind a self-declared birthday as its only primary age control, despite the same privacy policy stating the app 'is not directed to minors under 18.' Six further findings cover pre-consent SDK auto-init with no consent-management platform, voice capture routed to Tencent Cloud speech recognition, globally permitted cleartext traffic with no certificate pinning, a hardcoded Firebase API key, a Chinese OAID device-identifier harvesting stack feeding two attribution SDKs simultaneously, and a broad permission/overlay surface.

RFI-IRFOS disclosed all nine findings on 30 June 2026 to support@linke.ai, with the Austrian Datenschutzbehörde and the EDPS in BCC (moved to visible CC from the second message onward), stating an embargo of 28 September 2026. Every one of eight messages sent over the following 74 days (6 July, 17 July, 27 July, 5 August, 15 August, 31 August, 12 September 2026, plus the original) drew, within seconds to minutes, the identical automated support-desk acknowledgment: a thank-you template beginning 'Hi there, Thank you for reaching out to Linky Support' and stating the matter is 'currently being reviewed.' Not one of these eight replies engaged a single finding, cited a single GDPR article, or answered any of the three questions asked. This is not a silent case in the literal sense, eight replies were received, but it is a case of zero human engagement across 74 days and nine substantive messages.

The embargo of 28 September 2026 passed without any reply beyond the automated template. This report, published 19 days after that embargo, documents the full technical record together with the honest characterization of what Linky's responses actually were: present, identical, and content-free.

| ID | Severity        | Title                                                                                                                                                     |
|----|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| C1 | <b>CRITICAL</b> | Binary saturated with Chinese-origin SDKs and cloud endpoints (ByteDance, Mintegral, Tencent, Alibaba, ZEGO); China never disclosed in the privacy policy |
| C2 | <b>CRITICAL</b> | Ant Group/Alibaba 'Toyger'-class biometric face-liveness stack compiled in; vendor and PRC transfer undisclosed                                           |
| C3 | <b>HIGH</b>     | Sexual/romantic AI companion content ('Passion Mode') behind a self-declared-birthday age gate                                                            |

| ID | Severity | Title                                                                                                                                |
|----|----------|--------------------------------------------------------------------------------------------------------------------------------------|
| H1 | HIGH     | Pre-consent SDK auto-initialization; no consent-management platform; Facebook auto-collects the advertising identifier               |
| H2 | HIGH     | Voice capture routed to Tencent Cloud real-time speech recognition on a platform offering intimate conversation and live voice rooms |
| H3 | HIGH     | Cleartext traffic permitted globally; no certificate pinning on any domain including the app's own APIs; backup allowed              |
| H4 | HIGH     | Firebase/Google API key hardcoded in the distributed binary (project linkme-49e8a)                                                   |
| H5 | HIGH     | Chinese OAID device-identifier harvesting stack feeding two attribution SDKs and roughly ten ad networks simultaneously              |
| M1 | MEDIUM   | Broad permission, overlay, and accounts surface, plus an ad-SDK in-app APK install funnel                                            |

## Subject & Operator Context

Linky's published privacy policy names Skywork AI Pte. Ltd., Singapore, as the controller and governing-law jurisdiction. The app's production backend, domains, and native engine libraries evidence operation by USHOW Media (StarMaker codebase); the relationship between the declared controller and the operational backend is not clarified anywhere in the binary or the policy. No EU Art. 27 representative is named despite the app targeting EU users (a German locale split APK is present and one biometric endpoint is hosted in the EU-central region); no DPO is named. With no evidenced EU main establishment, there is no one-stop-shop lead authority; the Austrian Datenschutzbehoerde is the competent authority for this Austria-initiated disclosure.

## Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to support@linke.ai, the only contact address named in either the binary or the published privacy policy, with the Austrian Datenschutzbehoerde and the EDPS in BCC per standing practice (moved to visible CC from the 6 July follow-up onward), stating an embargo of 28 September 2026 and three specific questions on the undisclosed China transfers, the biometric face-liveness processing, and the age-assurance gap in front of sexual content.

Within seconds to minutes of that message, and of every one of the seven follow-ups that came after it (6 July, 17 July, 27 July, 5 August, 15 August, 31 August, 12 September 2026), support@linke.ai sent back a textually identical automated acknowledgment: a support-desk thank-you template stating the matter is being reviewed, with no reference to any finding, article, or question by name. All eight replies are word-for-word identical. At no point across 74 days and nine messages did a human respondent engage any of the nine findings or any of the three questions.

## Findings

**C1: Binary saturated with Chinese-origin SDKs and cloud endpoints (ByteDance, Mintegral, Tencent, Alibaba, ZEGO); China never disclosed in the privacy policy**

**CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:H/SI:N/SA:N, 9.1 — confirmed integration across advertising identifiers, analytics, stored media, and voice, routed to PRC-jurisdiction processors never named in the privacy policy**

```
Lcom/bytedance/sdk/openadsdk/... (Pangle v7.9.1.2, 5,427 refs)
Lcom/mbridge/msdk/... (Mintegral/Mobvista, 11,838 refs, Chinese-language UI strings)
Lcom/tencent/beacon/event/... + cos/xml + trtc + liteav + aai (Tencent Beacon/COS/TRTC/LiteAV/ASR)
libZegoLiveRoom.so (20.9MB, ZEGO real-time engine, Shenzhen)
cloudauth-intl.cn-hongkong.aliyuncs.com, cos.ap-shanghai.myqcloud.com, *.yunverify.com
Privacy policy (m.linke.ai/astro/policies/privacy/): no mention of China/PRC/any named vendor
```

**Impact:** The production binary embeds ByteDance Pangle (5,427 class references), Mintegral/Mobvista (11,838 references, shipping Chinese-language UI strings confirming live integration, not a stub), Tencent Beacon analytics, Tencent Cloud Object Storage, Tencent TRTC/LiteAV real-time audio/video, Tencent Cloud real-time speech recognition, Alibaba Cloud OSS storage and CloudAuth face verification, and ZEGO's real-time engine (a 20.9MB native library). Chinese cloud hostnames are hard-coded, including Hong Kong and Shanghai regions. The published privacy policy at m.linke.ai does not mention China, the PRC, or any of these vendors by name anywhere, stating only that data 'may be transferred to other jurisdictions where our affiliated entities are based.' Routing advertising identifiers, analytics events, stored media, and voice to Chinese-origin processors engages GDPR Chapter V (Art. 44, 46) and the PRC National Intelligence Law Art. 7, which compels Chinese organizations to assist state intelligence gathering; a Transfer Impact Assessment addressing this

exposure, if one exists, is not disclosed. Whether a given SDK is enabled in the live EU mediation waterfall and the precise runtime payloads is UNVERIFIED pending dynamic analysis; the integration, versioning, and endpoint wiring themselves are confirmed directly from the binary.

## C2: Ant Group/Alibaba 'Toyger'-class biometric face-liveness stack compiled in; vendor and PRC transfer undisclosed

**CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N, 9.0 — Art. 9 biometric data routed to an undisclosed, unnamed Chinese vendor via Hong Kong and EU-central endpoints**

```
libtoyger.so / libfacedevice.so / libIDVMNN.so / libdetector_core.so
Lcom/dtf/toyger/base/algorithm/ToygerLivenessConfig
faceBlinkLiveness, PhotinusLiveness, BatLiveness, Dragonfly_Liveness
cloudauth-intl-eu-central-1.yunverify.com, cloudauth-intl.cn-hongkong.aliyuncs.com
Privacy policy: "a one-time facial image through a third-party service... deleted
immediately" -- vendor and transfer not named
```

**Impact:** A full Ant Group/Alibaba 'Toyger/ZOLOZ'-class biometric face-liveness stack (libtoyger.so, libfacedevice.so, libIDVMNN.so; com.dtf.toyger; Dragonfly/Photinus/Bat liveness algorithms) is compiled into the app, with cloudauth/yunverify endpoints in Hong Kong and an EU-central region. The privacy policy discloses only: 'we may collect a one-time facial image through a third-party service. This data is deleted immediately after the check and will not be used for any other purpose' – it names neither the vendor nor that it is a Chinese provider, and does not address the international transfer of a facial image. Processing a facial image for liveness/age estimation is processing of biometric data for the purpose of uniquely identifying or assessing a natural person, an Art. 9(1) special category requiring an Art. 9(2) exemption, realistically only explicit consent here. The 'deleted immediately' claim cannot be verified from the client and is in tension with the existence of server-side cloudauth verification calls; no explicit-consent mechanism, retention proof, or Transfer Impact Assessment is disclosed.

### C3: Sexual/romantic AI companion content ('Passion Mode') behind a self-declared-birthday age gate

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:L/SA:N, 7.5 — downgraded from the original R1 finding's provisional CRITICAL label to the level its CVSS v4.0 vector supports; the underlying child-safety and Art. 8/9 concern is carried in full in the impact text and legal sections below regardless of the numeric score**

```
"Dive into sensual & intimate conversations. Unleash your fantasies with Passion Mode"
/api/user/nsfw/switch, RolePlayData, cp_Romantic,
  cp_Reach_LV_to_link_an_Intimate_Relationship
im_select_birthday, is_default_birthday, choose your age, is_minor, /api/match/
  minor_check
Privacy policy: "Linky is not directed to minors under the age of 18"
```

**Impact:** The app's core experience includes sexual/romantic AI conversation ('Passion Mode', an /api/user/nsfw/switch endpoint, intimate 'CP' relationship roleplay mechanics). The only primary age control evidenced in the binary is a self-declared birthday (im\_select\_birthday, is\_default\_birthday, choose your age) plus a server-side /api/match/minor\_check flag; there is no robust age-assurance mechanism in front of this content beyond self-declaration (C2's face check exists in the binary but its triggering condition and scope relative to NSFW access are not established statically). The privacy policy nonetheless states Linky 'is not directed to minors under the age of 18.' Conversation content of a sexual/romantic nature reveals data concerning a person's sex life or sexual orientation, an Art. 9(1) special category; a self-declared birthday is trivially defeated, meaning a minor can reach this content, engaging Art. 8 (conditions for a child's consent), Art. 25 (data protection by design), and a mandatory Art. 35 DPIA for large-scale special-category processing of intimate conversation. The gap between the policy's own claim and the actual gate is itself an Art. 5(2) accountability problem.

## H1: Pre-consent SDK auto-initialization; no consent-management platform; Facebook auto-collects the advertising identifier

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:L/SA:N, 7.1 — automatic on every launch, no CMP SDK integrated anywhere in the binary**

```
<provider android:name="com.google.firebase.provider.FirebaseInitProvider" android:
  directBootAware="true" android:initOrder="-2147483647"/>
<provider android:name="com.vungle.ads.VungleProvider" android:initOrder="102"/>
<meta-data android:name="com.facebook.sdk.AdvertiserIDCollectionEnabled" android:value
  ="true"/>
No integrated CMP SDK found (OneTrust/Didomi/Usercentrics/Sourcepoint each <=2 stray
  refs, no SDK)
```

**Impact:** Firebase (directBootAware), Facebook, Vungle, and Unity Ads all initialize via ContentProvider/Startup mechanisms at process start, before any consent UI can be shown. Facebook is explicitly configured with AdvertiserIDCollectionEnabled=true and AutoLogAppEventsEnabled=true. A search for integrated consent-management platforms (OneTrust, Didomi, Usercentrics, Sourcepoint) found only stray IAB-TCF read-key references used by ad SDKs to check an external consent string, not an integrated CMP of any kind; no SDK gates initialization behind consent anywhere in the binary.

## H2: Voice capture routed to Tencent Cloud real-time speech recognition on a platform offering intimate conversation and live voice rooms

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:H/SI:N/SA:N, 7.8 — confirmed SDK/library integration; live runtime transmission to the Chinese endpoint is UNVERIFIED pending dynamic analysis**

```
android.permission.RECORD_AUDIO, FOREGROUND_SERVICE_MICROPHONE
libqcloud_asr_realtime.so (Tencent Cloud real-time speech recognition)
Lcom/tencent/aai/..., Lcom/tencent/cloud/asr/..., Lcom/tencent/trtc/...,
  libZegoLiveRoom.so
```

**Impact:** The app holds RECORD\_AUDIO and microphone foreground-service permissions and ships Tencent Cloud real-time ASR (libqcloud\_asr\_realtime.so, com.tencent.aai, com.tencent.cloud.asr) alongside Tencent TRTC/LiteAV and ZEGO real-time audio engines. On a platform whose core function includes intimate/romantic AI conversation and live voice rooms, streaming captured voice to a Chinese cloud transcription service means voice content, which can itself reveal Art. 9 special categories, is processed by a PRC-jurisdiction processor, engaging Art. 9, Chapter V (Art. 44/46), and the same National Intelligence Law exposure as C1. That EU users' audio is in fact streamed to these endpoints at runtime is UNVERIFIED pending dynamic analysis; the SDK integration and permission wiring are confirmed directly from the binary.

### H3: Cleartext traffic permitted globally; no certificate pinning on any domain including the app's own APIs; backup allowed

**HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 7.3 — adjacent-network attacker on shared Wi-Fi/carrier infrastructure**

```
<application android:usesCleartextTraffic="true" android:allowBackup="true" .../>
<base-config cleartextTrafficPermitted="true"><trust-anchors><certificates src="system"
"/></trust-anchors></base-config>
No <pin-set> for any domain, including m.linke.ai, im-ws.linke.ai, api-track.linke.ai
```

**Impact:** usesCleartextTraffic="true" and a network-security-config base-config with cleartextTrafficPermitted="true" together permit unencrypted HTTP by default to every host except three explicitly listed exceptions (quantum-nexus.net, leadercc.com, cloudfront.net). No certificate pin-set exists for any domain, including the app's own API hosts (m.linke.ai, im-ws.linke.ai, api-track.linke.ai, \*.ushow.media). allowBackup="true" permits adb backup extraction of local app data, including an app whose local storage can contain intimate conversation history. A plaintext HTTP endpoint (image.cnamedomain.com) is present in the binary. Permitting cleartext and omitting pinning for a service carrying intimate conversation content falls short of the Art. 32(1)(a)/(b) state-of-the-art technical-measures standard.

### H4: Firebase/Google API key hardcoded in the distributed binary (project linkme-49e8a)

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 7.0 — availability/resilience finding, not a confidentiality finding (Firebase keys are not secrets by design)**

```
google_api_key / google_crash_reporting_api_key: [REDACTED IN PUBLIC REPORT --
disclosed privately to Skywork AI / Linky in R1]
project_id: linkme-49e8a
google_storage_bucket: linkme-49e8a.firebasestorage.app
```

**Impact:** The Firebase API key for project linkme-49e8a (also serving Crash Reporting) is hardcoded in res/values/strings.xml of every distributed copy of the app, extractable with apktool in under a minute. Firebase API keys are not confidentiality secrets by design, so the finding is one of availability and resilience under Art. 32(1)(b): an extracted key enables quota/billing exhaustion, and the burden is on the controller to confirm that Firebase Security Rules and the associated Cloud Storage bucket (linkme-49e8a.firebasestorage.app) are correctly locked to authenticated, deny-by-default access.

## H5: Chinese OAID device-identifier harvesting stack feeding two attribution SDKs and roughly ten ad networks simultaneously

**HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 7.1 — persistent OEM-mediated identifier, resists user reset**

```
com.asus.msa.SupplementaryDID.ACCESS, com.nemu.oaid.permission.read, freemme.  
permission.msa  
appsflyer (1,649 refs), adjust (835 refs) -- two attribution SDKs simultaneously  
Lcom/tencent/beacon/event (254 refs), facebook analytics (3,595 refs)  
bidmachine, moloco, ironsource, vungle, unity3d/ads, applovin, admob, inmobi
```

**Impact:** The app requests the OEM-specific permissions used by the Chinese Mobile Security Alliance's OAID SDK (ASUS MSA, nemu, freemme, Huawei common-data) to read a persistent device advertising identifier that resists a user's normal ad-ID reset. The binary simultaneously embeds two full attribution SDKs (AppsFlyer, 1,649 references; Adjust, 835 references), Tencent Beacon, Facebook analytics, and roughly ten ad-mediation networks (bidmachine, Moloco, ironSource, Vungle, Unity Ads, AppLovin, AdMob, InMobi, plus Pangle and Mintegral already covered in C1). A persistent, OEM-mediated identifier combined with dual attribution and heavy multi-network mediation enables cross-context behavioural profiling well beyond data-minimisation norms, and the Tencent Beacon path adds the same Chapter V exposure as C1.

## M1: Broad permission, overlay, and accounts surface, plus an ad-SDK in-app APK install funnel

**MEDIUM, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:R/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 4.0 — capability confirmed, not demonstrated misuse**

**Impact:** The app declares `SYSTEM_ALERT_WINDOW` (draw-over-other-apps), camera, microphone, coarse location, and multiple account-management permissions (`GET_ACCOUNTS`, `MANAGE_ACCOUNTS`, `AUTHENTICATE_ACCOUNTS`), and the Mintegral ad SDK ships an in-notification APK download/install UI, evidenced by embedded Chinese-language strings for 'download' and 'install.' Each of these widens the app's processing and attack surface and should be justified individually under Art. 5(1)(c) data minimisation and Art. 25; this is presented as a capability finding, not a demonstrated instance of misuse.

## Impact Analysis

---

Linky combines three independently serious patterns into one app: a China-saturated SDK and cloud footprint its own privacy policy never discloses as Chinese; a biometric face-liveness stack from an undisclosed, unnamed vendor; and sexual AI roleplay content protected by nothing more robust than a self-declared birthday. Each of these would warrant a CRITICAL or HIGH finding on its own; together, on a single app whose stated audience explicitly excludes minors, they describe a controller whose privacy documentation has not kept pace with its own architecture. The correspondence record compounds this: eight messages over 74 days drew eight identical automated acknowledgments and never once a human reply to any of it.

### **The Complete Chain: Eight Messages, 74 Days, Eight Identical Automated Replies, Zero Human Engagement**

---

Step 1 – Disclosure sent: RFI-IRFOS discloses nine findings on 30 June 2026 to support@linke.ai, BCC Austrian Datenschutzbehoerde and EDPS, stating an embargo of 28 September 2026. An automated acknowledgment arrives within 40 seconds.

Step 2 – Pattern established: Follow-ups on 6 July and 17 July 2026 each draw the identical automated template within seconds to minutes. The Austrian Datenschutzbehoerde and EDPS are moved to visible CC from 6 July onward.

Step 3 – Questions formally restated: A follow-up on 27 July 2026 places the three questions formally on record. The same automated template arrives.

Step 4 – Continued automation: Follow-ups on 5 August and 15 August 2026 restate the findings. Each draws the same identical template, now five and six times respectively.

Step 5 – 62 days, five canned replies: By 31 August 2026, RFI-IRFOS's own subject line names the pattern explicitly. The sixth identical template arrives the same day.

Step 6 – 74 days, zero substance: A final follow-up on 12 September 2026 draws the eighth identical automated reply.

Step 7 – Embargo passes: 28 September 2026, the stated embargo date, passes with no human reply ever received.

Step 8 – Publication: This report publishes 19 days after the embargo, documenting nine findings, eight messages, and eight identical automated replies that never once engaged a single one of them.

## Data Protection – Article by Article

---

Art. 44, 46, 35, 13(1)(f), 14 GDPR – Third-country transfer, DPIA, transparency: C1's Chinese-origin SDK and cloud saturation is undisclosed as Chinese anywhere in the privacy policy.

Art. 9, 44, 46, 35, 13, 14 GDPR – Special categories, third-country transfer: C2's biometric face-liveness stack processes Art. 9 data via an undisclosed, unnamed Chinese vendor.

Art. 9, 8, 25, 35, 5(2) GDPR – Special categories, conditions for a child's consent, DPIA, accountability: C3's sexual/romantic content sits behind a trivially defeated age gate, in tension with the app's own 'not directed to minors' claim.

Art. 6(1), 7(1), 5(1)(a), 5(2) GDPR; ePrivacy Art. 5(3) – Lawfulness, consent, storage/access: H1's pre-consent SDK auto-init with no CMP.

Art. 9, 44, 46, 5(1)(c) GDPR – Special categories, third-country transfer: H2's voice capture to Tencent Cloud ASR.

Art. 32(1)(a), 32(1)(b), 25 GDPR – Security of processing: H3's globally permitted cleartext traffic and absent certificate pinning.

Art. 32(1)(b), 25 GDPR – Security of processing: H4's hardcoded Firebase key.

Art. 5(1)(c), 6(1), 7, 25, 44 GDPR – Minimisation, lawfulness, third-country transfer: H5's Chinese OAID harvesting feeding dual attribution.

Art. 5(1)(c), 25 GDPR – Minimisation: M1's broad permission and overlay surface.

## Regulatory & Legal Landscape

---

Skywork AI Pte. Ltd. is a Singapore entity with no evidenced EU main establishment, meaning no one-stop-shop lead authority applies; the Austrian Datenschutzbehörde is the competent authority for this disclosure, with the EDPS copied throughout. No EU Art. 27 representative is named despite EU-directed distribution (a German-locale split APK and an EU-central biometric endpoint are both present in the binary), itself an independent Art. 27 gap. The absence of any DPO contact, combined with nine findings spanning Art. 8, 9, 13, 14, 25, 32, 35, 44, and 46, and zero human engagement across 74 days, describes a controller whose compliance posture has not been tested by this disclosure at all.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 9 issues in C2 and C3 and the Art. 44-46 third-country transfer issues in C1, C2, and H2, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 32 issues in H3 and H4, up to EUR 10,000,000 or 2% of total worldwide annual turnover.

## Indicators of Compromise

---

The following findings were extracted from static analysis of the production APK (base + arm64 split) using publicly available tooling (apktool, strings/grep over dex and the Dart libapp.so snapshot). No Linky/Skywork/USHOW servers, accounts, or infrastructure were probed; no dynamic instrumentation was performed. The hardcoded key referenced in H4 is withheld from this public report; full values were disclosed privately in the original R1 letter.

```
C1 -- Chinese SDK/cloud saturation (Pangle, Mintegral, Tencent, Alibaba, ZEG0); China
    undisclosed
C2 -- Ant/Alibaba Toyger-class biometric face-liveness; vendor and transfer
    undisclosed
C3 -- Sexual/romantic AI content behind self-declared-birthday age gate
H1 -- Pre-consent SDK auto-init, no CMP          H2 -- Voice capture to Tencent Cloud
    ASR
H3 -- Cleartext permitted globally, no pinning  H4 -- Hardcoded Firebase key, redacted
H5 -- Chinese OAIID harvesting + dual attribution M1 -- Broad permission/overlay
    surface
```

## Disclosure Timeline & Outcome

---

2026-06-30 Initial disclosure (nine findings) sent to support@linke.ai, BCC Austrian Datenschutzbehoerde and EDPS. Embargo stated as 2026-09-28. Automated acknowledgment arrives within 40 seconds.

2026-07-06 Follow-up sent, regulators moved to visible CC. Identical automated reply.

2026-07-17 Follow-up sent. Identical automated reply (second).

2026-07-27 Follow-up sent, three questions formally placed on record. Identical automated reply (third).

2026-08-05 Follow-up sent. Identical automated reply (fourth).

2026-08-15 Follow-up sent. Identical automated reply (fifth).

2026-08-31 Follow-up sent, 62 days, five canned replies noted explicitly in RFI-IRFOS's own subject line. Identical automated reply (sixth).

2026-09-12 Follow-up sent, 74 days, six identical replies noted. Identical automated reply (seventh/eighth overall, the last message in the thread).

2026-09-28 Embargo date reached and passed with zero human reply ever received.

2026-10-17 This report published, 19 days after the embargo. Correspondence record: eight RFI-IRFOS messages, eight identical automated support-desk replies, zero human engagement, zero of three questions answered.

## Residual Risk & Recommendations

---

C1 – Name every third-country processor (China specifically) and the applicable Art. 46 transfer mechanism and Transfer Impact Assessment in the privacy policy, for each SDK and cloud region actually enabled for EU users.

C2 – Name the biometric vendor explicitly, document the Art. 9(2) exemption and explicit-consent mechanism, and provide verifiable (not merely asserted) evidence of immediate deletion, ideally via an independent audit or published DPIA summary.

C3 – Implement an age-assurance mechanism for sexual/romantic content stronger than self-declared birthday, consistent with the app's own stated 'not directed to minors' policy, and document the Art. 8/9 lawful basis for processing intimate conversation content.

H1 – Integrate an actual consent-management platform and gate Firebase, Facebook, Vungle, and Unity Ads initialization behind it.

H2 – Disclose the Tencent Cloud ASR processing relationship and its legal basis explicitly, or replace it with an EU-processed alternative for EU users.

H3 – Extend certificate pinning to the app's own API domains and disable global cleartext permission.

H4 – Restrict and rotate the hardcoded Firebase key; confirm Security Rules and storage-bucket access are locked down.

H5 – Consolidate to a single attribution SDK and document the lawful basis for OAID collection specifically.

M1 – Review SYSTEM\_ALERT\_WINDOW, account-management permissions, and the ad-SDK install funnel against Art. 5(1)(c) minimisation.

Procedural: eight identical automated replies across 74 days, with zero human engagement on any finding, is itself a fact a supervisory authority may find relevant when assessing how this disclosure was handled internally. RFI-IRFOS remains open to a substantive reply to the three questions at any time; this report will be updated to reflect one if it arrives.

---

**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 All findings derive from static analysis of the published application (base APK + arm64 split) using publicly available tooling (apktool –no-src, strings/grep over dex and the Dart libapp.so snapshot). No Linky, Skywork AI, or USHOW Media servers, accounts, or infrastructure were probed; no dynamic instrumentation (Frida) was performed, consistent with RFI-IRFOS's R1-only static-analysis scope. The hardcoded credential referenced in finding H4 is withheld from this public report; the full value was disclosed privately in the original R1 letter and remains available to the controller or to a supervisory authority on request. Technical evidence is archived under chain of custody. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF LINKY-2026-R1-001.