



Security & Privacy Disclosure, Final Report

PolyBuzz / Speak Master (ai.socialapps.speakmaster)

An AI companion app fronted by a Delaware LLC routes captured voice, a pronunciation-scoring engine, and uploaded facial images to a Beijing-based real operator while the privacy policy names only the US and Singapore, is saturated with Chinese ad/analytics SDKs auto-initializing before any consent gate, gates 18+ content behind a self-declared birthday, and names no EU Art. 27 representative despite de-AT (Austrian) locale targeting, 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	Cloud Whale Interactive Technology LLC (Delaware, USA, published front) / 云游邦 (Beijing, PRC, real production operator, overseas brand "snapquiz")
Package	ai.socialapps.speakmaster (PolyBuzz: Chat with AI Friends, descended from the "Speak Master" language tutor)
Platform Audited	Android, static analysis of the production APK (base + arm64 + de splits, apktool/dex-strings/NSC/SDK-fingerprint)
Initial Disclosure (R1)	2026-06-30 (REF POLYBUZZ-2026-R1-001)
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	9 (3 Critical, 3 High, 3 Medium)
Correspondence	9 messages sent by RFI-IRFOS to support@mail.polybuzz.ai and shenyue03@zuoyebang.com over 68 days; zero reply of any kind, zero bounce, zero acknowledgment ever received
Authorities CC'd	Austrian Datenschutzbehoerde (DSB) · European Data Protection Supervisor (EDPS), both CC'd or BCC'd throughout

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: Chinese operator (Zuoyebang) behind a US/Singapore front: Chapter V transfer, China not disclosed	6
4.2	C2: Voice/speech pipeline: captured audio and a pronunciation engine route to the Chinese backend identified in C1	7
4.3	C3: Chinese and foreign ad/analytics SDK saturation auto-initialized pre-consent, with OAID harvesting	8
4.4	H1: 18+ companion content gated only by self-declared birthday, plus facial-image (biometric) upload	9
4.5	H2: Hardcoded Google/Firebase API key in strings.xml	9
4.6	H3: Cleartext traffic permitted globally in the production network security configuration	10
4.7	M1: Dangerous-permission over-collection for a chat/companion app	10
4.8	M2: No EU Art. 27 representative or DPO, despite de-AT (Austrian) locale targeting and Delaware governing law	11
4.9	M3: Attribution and analytics sprawl to multiple third countries via Alibaba Cloud OSS and Tencent COS	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

PolyBuzz (ai.socialapps.speakmaster, tens of millions of installs) presents to the public as a US product: the published developer is Cloud Whale Interactive Technology LLC, its Terms of Use are governed by Delaware law, and its privacy policy states chat data is stored on Singapore servers. A root-level static analysis of the production Android binary found a materially different story: the Android Application class is 'com.zuoyebang.appfactory.base.BaseApplication', file providers sit in the 'com.baidu.homework.*' namespace, and the production backend, crash/APM telemetry, analytics, and file-upload endpoints all resolve to Zuoyebang (字节跳动), a Beijing-based Chinese ed-tech company. None of this, nor China, is named anywhere in the published privacy policy (C1).

The app retains its origin as a language-tutor product: it holds RECORD_AUDIO, captures and MP3-encodes microphone audio, runs a Zuoyebang speech-evaluation/pronunciation-scoring native engine plus an on-device ONNX model, and exposes a server-side ASR (speech recognition) endpoint under the Zuoyebang-controlled backend, alongside custom-voice endpoints indicating voice-cloning or voice-selection features. Captured and potentially biometric-adjacent voice data is thereby routed to Chinese-controlled infrastructure with no disclosed Art. 44 safeguard (C2). The binary is additionally saturated with Chinese ad/analytics SDKs (ByteDance Pangle, Mintegral, BIGO Ads, Anythink/TopOn, Tencent Bugly/Mars/Cloud KMS/CLS) plus Chinese advertising-ID (OAID) harvesting, alongside Western mediation SDKs, all auto-initializing via ContentProviders at process start, before any consent dialog can appear; the one CMP present (Google UMP) runs only after these providers have already initialized (C3).

Three further HIGH findings compound the pattern: the app is an 18+ companion product with a "Pure Mode" toggle implying mature content exists, gated only by a self-declared, edit-once birthday, and it accepts an uploaded facial reference image to generate avatars, a biometric data point that, combined with C1, is exported to Chinese infrastructure (H1); a Google/Firebase API key is hardcoded in 'strings.xml' with no evident restriction (H2); and the production network security configuration permits cleartext traffic globally, with some analytics endpoints referenced over plain HTTP (H3). Three MEDIUM findings round out the picture: a dangerous-permission set (precise/coarse location, phone state, usage-stats, overlay) disproportionate for a chat app (M1); no EU Art. 27 representative or DPO despite a German locale split that specifically includes de-AT (Austrian) locales, establishing Austrian targeting under Art. 3(2) (M2); and an attribution/analytics recipient chain spanning Alibaba Cloud OSS and Tencent COS across the US, China, and Southeast Asia (M3).

RFI-IRFOS disclosed these findings on 30 June 2026 to support@mail.polybuzz.ai and the Zuoyebang-corporate contact shenyue03@zuoyebang.com, with the Austrian Datenschutzbehorde 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, 15 August, 31 August, 6 September 2026), each restating the findings and the three direct questions, moving the DSB and EDPS into CC from the second message onward. 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	Chinese operator (Zuoyebang) behind a US/Singapore front: Chapter V transfer, China not disclosed

ID	Severity	Title
C2	CRITICAL	Voice/speech pipeline: captured audio and a pronunciation engine route to the Chinese backend identified in C1
C3	CRITICAL	Chinese and foreign ad/analytics SDK saturation auto-initialized pre-consent, with OAID harvesting
H1	HIGH	18+ companion content gated only by self-declared birthday, plus facial-image (biometric) upload
H2	HIGH	Hardcoded Google/Firebase API key in strings.xml
H3	HIGH	Cleartext traffic permitted globally in the production network security configuration
M1	MEDIUM	Dangerous-permission over-collection for a chat/companion app
M2	MEDIUM	No EU Art. 27 representative or DPO, despite de-AT (Austrian) locale targeting and Delaware governing law
M3	MEDIUM	Attribution and analytics sprawl to multiple third countries via Alibaba Cloud OSS and Tencent COS

Subject & Operator Context

PolyBuzz presents a US/Singapore face (Cloud Whale Interactive Technology LLC, Delaware law, Singapore storage claim) while its production backend, APM telemetry, analytics, and file-upload infrastructure identify Zuoyebang (字节跳动), a Beijing-based Chinese ed-tech company known internationally as the "Baidu Homework" spin-off and overseas-branded "snapquiz", as the real operator. The app ships a German locale split that specifically includes de-AT (Austria), establishing EU and Austrian targeting.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to support@mail.polybuzz.ai and shenyue03@zuoyebang.com, BCC the Austrian Datenschutzbehörde and the European Data Protection Supervisor, stating an embargo date of 28 September 2026 under REF POLYBU ZZ-2026-R1-001. RFI-IRFOS followed up on 6 July, 17 July, 23 July, 31 July, 9 August, 15 August, 31 August, and 6 September 2026, moving the DSB and EDPS from BCC into CC from the second message onward. 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: Chinese operator (Zuoyebang) behind a US/Singapore front: Chapter V transfer, China not disclosed

CRITICAL (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7) — production backend and telemetry resolve to Beijing-based infrastructure while the privacy policy names only the US and Singapore

```
<application android:name="com.zuoyebang.appfactory.base.BaseApplication" ... >
launchable-activity: name='com.snapquiz.app.InitActivity'

https://api.polyspeak.ai/speakmaster/session/getsession
https://apm-volcano.zuoyebang.com (ByteDance Volcano Engine APM)
https://autotrack.zuoyebang.cc https://smt-upload.zuoyebang.com/uploader/v1/upload
https://sanxia.zybang.com https://www.zuoyebang.com
shenyue03@zuoyebang.com
```

Impact: The Android Application class is 'com.zuoyebang.appfactory.base.BaseApplication', the launcher activity is 'com.snapquiz.app.InitActivity', and a file provider sits in the 'com.baidu.homework.*' namespace. The production backend ('api.polyspeak.ai'), APM telemetry ('apm-volcano.zuoyebang.com'), analytics ('autotrack.zuoyebang.cc'), and a file-upload endpoint ('smt-upload.zuoyebang.com') all resolve to Zuoyebang (云鲸), a Beijing-based company, with an embedded developer contact at 'shenyue03@zuoyebang.com'. The published privacy policy frames the service as US (Cloud Whale Interactive Technology LLC, Delaware law) with chat storage on Singapore servers, and names neither Zuoyebang nor China anywhere.

C2: Voice/speech pipeline: captured audio and a pronunciation engine route to the Chinese backend identified in C1

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, 8.0) — RFI-IRFOS blast-radius escalation: raised to CRITICAL because voice is biometric-adjacent personal data routed to a third country with no disclosed Art. 44 safeguard, not because a specific voiceprint was extracted or misused

```
android.permission.RECORD_AUDIO    android.permission.MODIFY_AUDIO_SETTINGS
android/media/AudioRecord    startRecording
lib/arm64-v8a/libmp3lame.so    lib/arm64-v8a/libzms_engine_jni_new.so    lib/arm64-v8a/
    libonnxruntime.so

/speakmaster/conversation/asr    /speakmaster/conversation/record    /speakmaster/
    conversation/localrecord
/speakmaster/page/customVoiceNew/index    /speakmaster/page/switchVoice/index
https://smt-upload.zuoyebang.com/uploader/v1/upload
```

Impact: The app holds RECORD_AUDIO and MODIFY_AUDIO_SETTINGS, captures audio via 'android.media.AudioRecord'/'startRecording', MP3-encodes it, and runs a native Zuoyebang speech-evaluation/pronunciation-scoring engine alongside an on-device ONNX runtime. A server-side ASR (automatic speech recognition) endpoint exists under the operator backend ('/speakmaster/conversation/asr'), alongside recording, local-record, and custom-voice endpoints. Spoken audio and any derived pronunciation/voice profile are personal data and biometric-adjacent; routing it to the Chinese-controlled infrastructure identified in C1 is a Chapter V transfer with no disclosed safeguard, and the large-scale, systematic nature of voice processing in a companion/tutor app would ordinarily require a documented Art. 35 DPIA.

C3: Chinese and foreign ad/analytics SDK saturation auto-initialized pre-consent, with OAID harvesting

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 Chinese-origin ad/analytics SDKs initialize before any consent gate across tens of millions of installs, re-raising the Art. 44 transfer issue independent of the core backend, not because a specific exploit of the auto-init mechanism was demonstrated

```
5705 ByteDance Pangle (com/bytedance/sdk/openadsdk) 9579 Mintegral/Mobvista (com/
mbridge/msdk)
5125 BIGO Ads (sg/bigo/ads) 646 Tencent Bugly ~50 OAID (MSA/miitmdid)
5867 AppLovin 7274 Unity Ads 7244 ironSource 6036 Moloco 1589 AppsFlyer

com.applovin.sdk.AppLovinInitProvider sg.bigo.ads.controller.provider.
BigoAdsProvider
com.tencent.rmonitor.launch.AppLaunchMonitorInstaller com.secmtv.sdk.core.api.
ATInitializationProvider

uses-permission: com.google.android.gms.permission.AD_ID,
ACCESS_AD SERVICES_ATTRIBUTION/AD_ID/TOPICS
```

Impact: Multiple Chinese-origin ad/analytics SDKs (ByteDance Pangle, Mintegral/Mobvista, BIGO Ads, Anythink/TopOn, Tencent Bugly/Mars/Cloud KMS/CLS) plus Chinese advertising-ID (OAID) harvesting are compiled into the app alongside Western mediation SDKs (AppLovin, Unity Ads, ironSource, Moloco, Vungle, Tapjoy, adjoie, AppsFlyer). Their initialization providers (AppLovinInitProvider, MobileAdsInitProvider, FacebookInitProvider, MBComponentLifecycleProvider, BigoAdsProvider, VungleProvider, BidMachineInitProvider, Tramini ContentProvider, adjoie's DatabaseContentProvider, Tencent's AppLaunchMonitorInstaller) fire automatically at application process start, before any consent UI. A Google UMP consent platform is present but runs only after these providers have already initialized.

H1: 18+ companion content gated only by self-declared birthday, plus facial-image (biometric) upload

HIGH (CVSS v4.0 AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.1) — mature content and avatar-generation from an uploaded face image, defeated by any self-declared birth date

```
age_incompatibility_tips: "Sorry, this app is only available for users aged 18 and above."
birthday_changed_once_desc_new: "Select a birth date (18+ only). Once set, it cannot be edited."
avatar_reference_explain: "Generate Avatar based on uploaded facial reference image."
agreement_age_level_lower_desc: "Show Pure Mode Content"
```

Impact: The app is an 18+ AI-companion product with a "Pure Mode" toggle implying non-pure (mature) content exists. The only age control is a self-declared, edit-once birthday, trivially entered falsely by any user. The app separately accepts an uploaded facial reference image to generate an AI avatar, a biometric data point under Art. 9 that, combined with C1's Chinese infrastructure, is exported to a jurisdiction with no disclosed transfer safeguard.

H2: Hardcoded Google/Firebase API key in strings.xml

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, 5.3) — extractable credential with no evidence of API-side restriction

```
google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to PolyBuzz/
  Zuoyebang in R1]
google_app_id: 1:690919060741:android:c390b293b6efee461f336c
project_id: speakmaster-ac9b3
```

Impact: A Google/Firebase API key is extractable verbatim from 'res/values/strings.xml' in the production build, with no evidence of referrer, app-signature, or quota restriction. Under Art. 32 the burden is on the operator to demonstrate the key is scoped; absent that evidence, an extractable key is a quota/billing-exhaustion and potential data-exposure vector.

H3: Cleartext traffic permitted globally in the production network security configuration

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, with some endpoints referenced over plain HTTP

```
<base-config cleartextTrafficPermitted="true">
  <trust-anchors><certificates src="system" /></trust-anchors>
</base-config>
<debug-overrides cleartextTrafficPermitted="true">
  <trust-anchors><certificates src="system" /><certificates src="user" /></trust-anchors>
</debug-overrides>
```

Impact: The production 'base-config' in the network security configuration permits cleartext (HTTP) traffic to any host, and some embedded analytics/tracking endpoints are referenced over 'http://'. No certificate-pinning configuration is present for the app's own domains. For an app that transmits voice, chat, and identifiers, global cleartext permission is a meaningful interception risk.

M1: Dangerous-permission over-collection for a chat/companion app

MEDIUM (CVSS v4.0 AV:P/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.6) — location, phone-state, usage-stats, and overlay permissions with no disclosed purpose

```
android.permission.ACCESS_FINE_LOCATION    android.permission.ACCESS_COARSE_LOCATION
android.permission.READ_PHONE_STATE        android.permission.PACKAGE_USAGE_STATS
android.permission.SYSTEM_ALERT_WINDOW     android.permission.WRITE_SETTINGS
```

Impact: The manifest requests ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, READ_PHONE_STATE, PACKAGE_USAGE_STATS, SYSTEM_ALERT_WINDOW, and WRITE_SETTINGS. These exceed what an AI-chat/companion product needs and are consistent with the ad/analytics saturation documented in C3; each permission must have an Art. 6 lawful basis and satisfy data minimisation.

M2: No EU Art. 27 representative or DPO, despite de-AT (Austrian) locale targeting and Delaware governing law

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 blocking EU data subjects and supervisory authorities from identifying a responsible controller

```
split_config.de.apk -> locales: 'de' 'de-AT' 'de-DE'  
Terms of Use: governed by the law of the State of Delaware, USA  
EU Art. 27 representative: NONE found in binary or published policy  
DPO: NONE found
```

Impact: The German locale split ships 'de', 'de-DE', and specifically 'de-AT' (Austrian) locales, establishing targeting of Austrian data subjects under Art. 3(2). The operator front is a Delaware LLC and the real operator is based in Beijing; no EU Art. 27 representative and no DPO are named in the binary or the published Terms/Policy. Given the large-scale voice processing in C2, an Art. 37 DPO appointment is likely required.

M3: Attribution and analytics sprawl to multiple third countries via Alibaba Cloud OSS and Tencent COS

MEDIUM (CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.0) — undisclosed recipient chain spanning the US, China, and Southeast Asia

```
ad-host-backup-europe.oss-eu-central-1.aliyuncs.com  
ad-host-backup-asia.oss-ap-southeast-1.aliyuncs.com  
cos-android-sdk-doc-1253960454.cos.ap-shanghai.myqcloud.com/beacon_cc/android/
```

Impact: Beyond the core backend and ad/analytics SDKs in C1 and C3, attribution and ad-configuration data flows to Alibaba Cloud OSS (including an EU-region bucket alongside Shanghai/Southeast Asia buckets) and Tencent Cloud Object Storage hosted in Shanghai. Each additional recipient and transfer in this chain must be disclosed under Art. 13/14 and governed by Art. 28 processor terms; none of this chain is named in the published privacy policy.

Impact Analysis

C1, C2, and C3 form a single pattern: a Delaware LLC front names only the US and Singapore while the real operator, Zuoyebang in Beijing, receives the production backend traffic (C1), the captured voice and pronunciation data (C2), and sits alongside a saturation of Chinese ad/analytics SDKs that initialize before consent (C3). H1 through H3 and M1 through M3 are the mechanics and gaps underneath: a trivially defeated age gate in front of mature content and biometric facial uploads, a hardcoded credential, insecure transport, permission over-collection, no EU representative despite explicit Austrian targeting, and a wider undisclosed third-country storage chain.

What ties all nine findings together procedurally is the correspondence record: nine messages, sent to two named, functioning addresses 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 support@mail.polybuzz.ai and shenyue03@zuoyebang.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, 15 August, and 31 August 2026, each restating the three direct questions and the days elapsed, moving the DSB and EDPS into CC from the second message onward. 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 two functioning addresses, the correspondence record contains zero replies of any kind.

Data Protection – Article by Article

Art. 44-49, 13(1)(f), 14(1)(f), 5(1)(a), 6 GDPR – Third-country transfer, recipient disclosure, transparency: C1's backend and telemetry resolve to Beijing while the policy names only the US and Singapore.

Art. 9, 44, 5(1)(c), 6, 7, 35 GDPR – Special/biometric-adjacent category data, transfer, minimisation, lawful basis, DPIA: C2's voice capture and ASR pipeline reaches the Chinese backend identified in C1.

Art. 6(1), 7, 5(1)(a)/(c), 25, 44 GDPR – Lawful basis, valid consent, data protection by design: C3's pre-consent SDK auto-initialization, including Chinese-origin SDKs.

Art. 8, 9, 25 GDPR – Child consent/age assurance, biometric data: H1's self-declared age gate in front of mature content and facial-image uploads.

Art. 32 GDPR – Security of processing: H2's hardcoded, apparently unrestricted API credential.

Art. 32, 5(1)(f) GDPR – Security and integrity/confidentiality: H3's globally cleartext-permitting production transport configuration.

Art. 5(1)(c), 6 GDPR – Data minimisation: M1's disproportionate permission set.

Art. 27, 37, 3(2) GDPR – EU representative, DPO, territorial scope: M2's absence of any EU representative despite Austrian locale targeting.

Art. 13, 14, 44, 26, 28 GDPR – Recipient and transfer disclosure, processor terms: M3's undisclosed third-country storage chain.

Regulatory & Legal Landscape

Cloud Whale Interactive Technology LLC (Delaware) and the real operator, Zuoyebang (Beijing, PRC), have no EU main establishment and no Art. 27 representative, so no one-stop-shop mechanism applies. RFI-IRFOS's lead reporting authority for this case is the Austrian Datenschutzbehörde (DSB), given the explicit de-AT Austrian locale targeting, informed in BCC on the initial disclosure and in CC on every subsequent follow-up, alongside the European Data Protection Supervisor, under GDPR Art. 83(2)(b).

Fine exposure under GDPR: Art. 83(5) applies to the Art. 44-49 transfer issues in C1 and C2, the Art. 6/7/25/44 pre-consent and SDK transfer issue in C3, and the Art. 8/9 minors/biometric issue in H1, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Art. 83(4) applies to the Art. 32 and 5(1)(c)/27/37 issues in H2, H3, M1, M2, and M3, up to EUR 10,000,000 or 2% of total worldwide annual turnover. An operator with tens of millions of installs 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 Zuoyebang, Tencent, Alibaba, or related servers, accounts, or infrastructure were probed.

```
C1 -- com.zuoyebang.appfactory.base.BaseApplication, api.polyspeak.ai, apm-volcano.
    zuoyebang.com

C2 -- RECORD_AUDIO, libzms_engine_jni_new.so, /speakmaster/conversation/asr

C3 -- ByteDance Pangle, Mintegral, BIGO Ads, Anythink/TopOn, Tencent Bugly/Mars/KMS/
    CLS, OAID

H1 -- age_incompatibility_tips, avatar_reference_explain strings (strings.xml)

H2 -- google_api_key in strings.xml (redacted above)

H3 -- network_security_config.xml: cleartextTrafficPermitted="true" in base-config

M1 -- ACCESS_FINE_LOCATION, READ_PHONE_STATE, PACKAGE_USAGE_STATS, SYSTEM_ALERT_WINDOW

M2 -- split_config.de.apk locales 'de' 'de-AT' 'de-DE'; no Art. 27 rep, no DPO in
    binary or policy

M3 -- ad-host-backup-europe.oss-eu-central-1.aliyuncs.com, cos-android-sdk-doc
    -1253960454.cos.ap-shanghai.myqcloud.com
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to support@mail.polybuzz.ai and shenyue03@zuoyebang.com, BCC Austrian DSB and EDPS. Embargo stated as 2026-09-28. REF POLYBUZZ-2026-R1-001.

2026-07-06, 2026-07-17, 2026-07-23, 2026-07-31, 2026-08-09, 2026-08-15, 2026-08-31
Seven follow-up messages, each restating the nine findings and the three direct questions, with the DSB and EDPS moved into CC from the second message onward. 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: disclose the Zuoyebang/China processing chain in the privacy policy and document an Art. 46 transfer safeguard and transfer-impact assessment.

C2 – Immediate: document the lawful basis and transfer safeguard for voice data reaching the Zuoyebang-controlled ASR backend, and complete the Art. 35 DPIA for large-scale voice processing.

C3 – Immediate: gate all advertising/analytics SDK initialization, not only AdMob, behind a consent management platform before any provider initializes.

H1 – Near-term: replace the self-declared birthday gate with verified age assurance in front of mature content, and document the Art. 9 basis for facial-image processing.

H2 – Near-term: rotate and restrict the hardcoded Google/Firebase API key.

H3 – Near-term: disable global cleartext in the production network security configuration and migrate remaining HTTP endpoints to TLS.

M1 – Near-term: remove or justify the location, phone-state, usage-stats, and overlay permissions.

M2 – Near-term: designate a written Art. 27 EU representative and a DPO under Art. 37, given the explicit de-AT targeting.

M3 – Near-term: disclose the full third-country attribution/storage recipient chain and document Art. 28 processor terms for each recipient.

Across all findings: establish a monitored intake path for security and data-protection disclosures sent to support@mail.polybuzz.ai and shenyue03@zuoyebang.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 • Elisabethinergasse 25/10, 8020 Graz, Austria All findings derive from static analysis of the published application using publicly available tooling. No Zuoyebang, Tencent, Alibaba, or related 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 POLYBUZZ-2026-R1-001.