



Security & Privacy Disclosure, Final Report

Saylo / AI Character Story Chat (com.xverse.aistory)

An AI companion app with 5M+ installs routes login, chat, and LLM data to Chinese infrastructure while its privacy policy claims only anonymized data leaves the device, offers intimate/romantic AI conversation behind a self-declared birthday field, and names no EU Art. 27 representative or DPO despite shipping a German locale split, unresolved through eight 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, EIGHT FINDINGS REMAIN UNADDRESSED**

Target	X Original (Hong Kong) Limited (published developer) / XVERSE Technology (Shenzhen, PRC) (backend operator)
Package	com.xverse.aistory (Saylo / "AI Character Story Chat", consumer domain sayloai.com)
Platform Audited	Android, static analysis of the production APK (base + arm64 + de splits, apktool/dex-strings/Hermes-bundle/NSC/SDK-finger print)
Initial Disclosure (R1)	2026-06-30 (REF SAYLO-2026-R1-001)
Disclosure / Embargo Date	2026-09-28
Report Published	2026-10-17
Overall Severity	CRITICAL
Findings	8 (3 Critical, 3 High, 2 Medium)
Correspondence	8 messages sent by RFI-IRFOS to saylo@xverse.cn and support@sayloai.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 and infrastructure saturation: login, chat, LLM, analytics, and ad SDKs all resolve to PRC/Hong Kong processors, undisclosed	6
4.2	C2: Intimate/romantic AI companion content behind a self-declared birthday field, reaching a PRC LLM backend	7
4.3	C3: No EU Art. 27 representative, no DPO, and no identified controller address, despite established EU targeting	8
4.4	H1: Advertising and analytics SDKs auto-initialize before any consent gate; the one consent surface present does not cover them	9
4.5	H2: Insecure transport: cleartext permitted globally, user CAs trusted in production, login API over plain HTTP	10
4.6	H3: Hardcoded Google/Firebase API key and Facebook client token in strings.xml	10
4.7	M1: High-density ad mediation and cross-device attribution alongside phone-state/IMEI device-ID harvesting	11
4.8	M2: Microphone, camera, and WebRTC voice capture in an intimate AI-companion context	11
5	Impact Analysis	12
6	The Complete Chain: Eight 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

Saylo (com.xverse.aistory, ~5M+ Play installs) is an AI character / companion story-chat app published by X Original (Hong Kong) Limited, a front for XVERSE Technology (Shenzhen, PRC), whose backend serves the app from 'xverse.cn' infrastructure. A root-level static analysis of the production Android binary (base + arm64 + German-locale splits) found eight findings, three CRITICAL, three HIGH, and two MEDIUM.

The app's entire production backend, including the login and chat API, LLM data collection, asset hosting, and a Tencent EdgeOne proxy fleet, resolves to Chinese infrastructure under '*.xverse.cn', including a Shanghai-hosted asset endpoint. Behavioral analytics routes to Sensors Analytics (a Chinese analytics platform), and crash/performance telemetry routes to Tencent. The binary also embeds ByteDance Pangle, Mintegral, Sensors Analytics, and BIGO Ads, alongside Alibaba Cloud OSS storage with an EU-region bucket. None of this is disclosed: the published privacy policy states that "only aggregated, anonymized data is periodically transmitted to external services" and never mentions China, XVERSE, Sensors, Tencent, ByteDance, or Alibaba (C1). Separately, the app offers an intimate/romantic AI companion chat mode ('CHAT_MODE_INTIMATE', 'isNsfw') that can surface content concerning a user's sex life, data that constitutes a special category under GDPR Art. 9, behind nothing more than a self-declared birthday field and an optional password-protected "Teen Mode" toggle, while the privacy policy claims the service is not directed to under-18s (C2). The operator, established in Hong Kong and Shenzhen, names no EU Art. 27 representative and no Data Protection Officer anywhere in the binary or the published privacy policy, despite shipping a German-locale split, German UI strings, and EU-region attribution and cloud storage that together establish EU targeting (C3).

Three further HIGH findings compound the pattern: advertising and analytics SDKs (Sensors Analytics, BIGO Ads, Facebook, AppLovin, AdMob, ironSource, Vungle, Firebase) auto-initialize via ContentProviders at process start, before any consent gate, and the one consent surface present (Google UMP) governs only AdMob, not the others (H1); the production network security configuration permits cleartext traffic globally and trusts user-installed CAs in the base config rather than confining that trust to debug builds, with the login/LLM API itself reachable over plain HTTP (H2); and a Google/Firebase API key plus a Facebook client token are hardcoded in 'strings.xml' with no evident restriction (H3). Two MEDIUM findings round out the picture: eight or more ad-mediation SDKs plus two attribution SDKs alongside 'READ_PHONE_STATE'/IMEI access (M1), and microphone/camera/WebRTC voice-chat capability in an intimate-companion context with the transmission destination of captured audio unverified (M2).

RFI-IRFOS disclosed these findings on 30 June 2026 to saylo@xverse.cn and support@sayloai.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 seven further messages (6 July, 17 July, 23 July, 31 July, 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 eight 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 and infrastructure saturation: login, chat, LLM, analytics, and ad SDKs all resolve to PRC/Hong Kong processors, undisclosed
C2	CRITICAL	Intimate/romantic AI companion content behind a self-declared birthday field, reaching a PRC LLM backend
C3	CRITICAL	No EU Art. 27 representative, no DPO, and no identified controller address, despite established EU targeting
H1	HIGH	Advertising and analytics SDKs auto-initialize before any consent gate; the one consent surface present does not cover them
H2	HIGH	Insecure transport: cleartext permitted globally, user CAs trusted in production, login API over plain HTTP
H3	HIGH	Hardcoded Google/Firebase API key and Facebook client token in strings.xml
M1	MEDIUM	High-density ad mediation and cross-device attribution alongside phone-state/IMEI device-ID harvesting
M2	MEDIUM	Microphone, camera, and WebRTC voice capture in an intimate AI-companion context

Subject & Operator Context

Saylo is an AI character / companion story-chat app published under the name "X Original" (Hong Kong) for app-store purposes, while its production backend, LLM inference, and operator contact (saylo@xverse.cn) identify 限有 XVERSE Technology, headquartered in Shenzhen, China, as the actual operator. The app ships a German locale split and EU-region attribution and cloud storage, establishing that it is offered to EU data subjects.

Engagement Summary

RFI-IRFOS sent the initial disclosure on 30 June 2026 to saylo@xverse.cn and support@sayloai.com, BCC the Austrian Datenschutzbehörde and the European Data Protection Supervisor, stating an embargo date of 28 September 2026 under REF SAYLO-2026-R1-001. RFI-IRFOS followed up on 6 July, 17 July, 23 July, 31 July, 15 August, 31 August, and 6 September 2026, moving the DSB and EDPS from BCC into CC from the second message onward. Eight 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 and infrastructure saturation: login, chat, LLM, analytics, and ad SDKs all resolve to PRC/Hong Kong processors, undisclosed

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) — login, chat, and LLM conversation content routes to Chinese infrastructure while the privacy policy denies any such transfer

```
http://core-api.xverse.cn/api/login_service/...
http://core-api.xverse.cn/api/llm_login_service/...
https://prd-collect-llm.xverse.cn https://media.xverse.cn https://schedule.xverse.
cn
https://asset-sh.xverse.cn (sh = Shanghai) https://edgeone-prd-yunjing-proxy.xverse.
cn (Tencent EdgeOne)
https://sayloai.datasink.sensorsjourney.com/sa (Sensors Analytics, Chinese)
beacon.qq.com aegis.qq.com btrace.qq.com mplog.qq.com (Tencent telemetry)
ad-host-backup-europe.oss-eu-central-1.aliyuncs.com (Alibaba Cloud OSS, EU region)
Lcom/bytedance/sdk/openadsdk (ByteDance Pangle, 2,319 refs) Lcom/mbridge/msdk (
Mintegral, 3,567 refs)
```

Privacy policy (verbatim): "Only aggregated, anonymized data is periodically transmitted to external services." -- never mentions China, XVERSE, Sensors, Tencent, ByteDance, or Alibaba.

Impact: The login API, chat API, LLM data-collection endpoint, asset hosting, and a Tencent EdgeOne CDN proxy all resolve to '*.xverse.cn', including a Shanghai-hosted asset host. Behavioral analytics routes to Sensors Analytics (a Chinese analytics platform) and crash/performance telemetry routes to Tencent '*.qq.com'. The binary embeds ByteDance Pangle, Mintegral, Sensors Analytics, and BIGO Ads, and uses Alibaba Cloud OSS storage including an EU-region bucket. The published privacy policy states that only aggregated, anonymized data leaves the device and never names China, XVERSE, Sensors, Tencent, ByteDance, or Alibaba, directly contradicting the binary-confirmed per-user API and analytics traffic to these processors.

C2: Intimate/romantic AI companion content behind a self-declared birthday field, reaching a PRC LLM backend

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, 7.8) — RFI-IRFOS blast-radius escalation: raised from a HIGH-band technical score to CRITICAL because the age gate is trivially defeated at the scale of a 5M+-install consumer app, exposing minors to Art. 9 special-category content processed by a Chinese LLM, not because active exploitation of a minor's account was observed

```
CHAT_MODE_INTIMATE  isNsfw  Romantic  sexual / Sexual  explicit / Explicit  18+
  flirt
birthday / Birthday  Minor / minor  coppa / CopPa  harmful_to_minors
  video_review_rejected_minor
setTeenModePassword  verifyTeenModePassword  resetTeenModePassword
```

Privacy policy (verbatim): "The Service Provider does not knowingly collect personally identifiable information from children under 18 years of age."

Impact: The app exposes an intimate/romantic chat mode ('CHAT_MODE_INTIMATE') and an NSFW flag ('isNsfw'). Romantic/sexual conversation content reveals data concerning a person's sex life or sexual orientation, a special category under GDPR Art. 9. The only evidenced age controls are a self-declared 'birthday' field and an optional, password-protected "Teen Mode" toggle, both trivially defeated by any user willing to enter a false birth date. The conversation content itself is processed by the Chinese LLM backend identified in C1, compounding the special-category exposure with an undisclosed third-country transfer.

C3: No EU Art. 27 representative, no DPO, and no identified controller address, despite established EU targeting

CRITICAL (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, 5.3) — RFI-IRFOS blast-radius escalation: raised from a structural-accountability-only technical score to CRITICAL because it is the entry point blocking any EU data subject or supervisory authority from identifying a responsible controller, not because of a direct technical exploit

```
split_config.de.apk -> badging: split='config.de', locales: 'de' 'de-DE'
Hermes bundle German UI strings: "Saylo-Android-Nutzer", "Willkommen", "Absenden", "
    Storno", "Mehr"
Adjust attribution (EU): subscription.eu.adjust.com, ssrv.eu.adjust.com
Alibaba OSS (EU region): ad-host-backup-europe.oss-eu-central-1.aliyuncs.com

Privacy policy: Service Provider named only as "X original" -- no company address, no
    DPO, no Art. 27 representative, sole contact support@sayloai.com
```

Impact: The app ships a German locale split, German UI strings, EU-region Adjust attribution endpoints, and an EU-region Alibaba Cloud OSS bucket, together establishing that the app offers services to EU data subjects. The operator is established in Hong Kong and Shenzhen, outside the EU. No Art. 27 representative and no Data Protection Officer are named anywhere in the binary or the published privacy policy, which names the Service Provider only as "X original" with no company address. A controller outside the EU offering services to EU data subjects must designate a written Art. 27 representative in the Union, and given the large-scale special-category processing in C2 and the systematic ad/analytics monitoring in H1 and M1, must appoint a DPO under Art. 37(1)(b)/(c).

H1: Advertising and analytics SDKs auto-initialize before any consent gate; the one consent surface present does not cover them

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)
— Sensors Analytics, BIGO, Pangle, and Facebook initialize at process start with no consent gate in front of them

```
<provider android:name="com.sensorsdata.analytics.android.sdk.data.
  SensorsDataContentProvider".../>
<provider android:name="sg.bigo.ads.controller.provider.BigoAdsProvider"/>
<provider android:name="com.facebook.internal.FacebookInitProvider"/>
<provider android:name="com.applovin.sdk.AppLovinInitProvider"/>
<provider android:name="com.google.android.gms.ads.MobileAdsInitProvider"/>
<provider android:name="com.ironsource.lifecycle.IronsourceLifecycleProvider"/>
<provider android:name="com.vungle.ads.VungleProvider"/>
<provider android:name="com.google.firebase.provider.FirebaseInitProvider"
  directBootAware="true"/>

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

CMP search: only com.google.android.ump present (61 refs, AdMob-only); no OneTrust/
Didomi/Usercentrics/Sourcepoint SDK
```

Impact: Sensors Analytics, BIGO Ads, Facebook, AppLovin, AdMob, ironSource, Vungle, and Firebase all initialize via ContentProvider or Startup at application process start, before any consent UI can appear. The app holds the AD_ID permission and the full ACCESS_AD_SERVICES permission set. A search for integrated Consent Management Platforms found only Google UMP (61 references), which gates AdMob ads only; it does not gate the Sensors, BIGO, Pangle, or Facebook providers that auto-initialize regardless.

H2: Insecure transport: cleartext permitted globally, user CAs trusted in production, login API over plain HTTP

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, 6.8)
— production network security config trusts user-installed CAs and permits cleartext traffic globally

```
<base-config cleartextTrafficPermitted="true">
  <trust-anchors>
    <certificates src="system" />
    <certificates src="user" /> <!-- user CAs trusted in PRODUCTION base-config -->
  </trust-anchors>
</base-config>

android:allowBackup="true"    android:extractNativeLibs="true"
http://core-api.xverse.cn/api/... (login + LLM swagger references over plain HTTP)
```

Impact: The production network security configuration's 'base-config' permits cleartext traffic globally and adds user-installed CAs to its trust anchors, not confined to a '<debug-overrides>' block. No certificate pinning is configured for the app's own '*.xverse.cn' domains. The login and LLM API is referenced with an 'http://' scheme, and 'android:allowBackup="true"' additionally permits extraction of app data via ADB backup on many devices.

H3: Hardcoded Google/Firebase API key and Facebook client token 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 credentials with no evidence of API-side restriction

```
google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Xverse in R1]
google_crash_reporting_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately to Xverse in R1]
google_app_id: 1:881520035018:android:96c3e8798baf87d2326033
facebook_app_id: 3574470669521609
facebook_client_token: [REDACTED IN PUBLIC REPORT -- disclosed privately to Xverse in R1]
```

Impact: A Google/Firebase API key (reused for both the general API key and the crash-reporting key) and a Facebook client token are extractable verbatim from 'res/values/strings.xml' in the production build, with no evidence of referrer, app-signature, or quota restriction on either. Under Art. 32 the burden is on the operator to demonstrate the keys are scoped; absent that evidence, an extractable key is a quota/billing-exhaustion and potential data-exposure vector.

M1: High-density ad mediation and cross-device attribution alongside phone-state/IMEI device-ID harvesting

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, 4.2) — eight-plus ad SDKs and two attribution SDKs alongside disproportionate device-identifier access

Ad mediation: AppLovin (3,059) Unity Ads (4,657) ironSource (3,812) Vungle (1,291)
 ByteDance Pangle (2,319) Mintegral (3,567) BIGO Ads Tapjoy
 Chartboost (22)
 Attribution: AppsFlyer (794) Adjust (226)
 Device IDs: READ_PHONE_STATE + getDeviceId / getImei / TelephonyManager references

Impact: The app embeds at least eight ad-mediation SDKs (AppLovin, Unity Ads, ironSource, Vungle, ByteDance Pangle, Mintegral, BIGO Ads, Tapjoy, Chartboost) plus two cross-platform attribution SDKs (AppsFlyer, Adjust), holds 'READ_PHONE_STATE', and references 'getImei'/'getDeviceId'/'TelephonyManager' alongside advertising and Android ID collection. Persistent device-identifier access on a modern target SDK is disproportionate for an AI-chat app and engages Art. 5(1)(c) data minimisation.

M2: Microphone, camera, and WebRTC voice capture in an intimate AI-companion context

MEDIUM (CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 3.9) — voice/video capability with the destination of captured audio unverified

android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.
 MODIFY_AUDIO_SETTINGS
 android.permission.READ_MEDIA_AUDIO / _IMAGES / _VIDEO
 Hermes bundle: setSpeakerphoneOn, setSpeakingVideoUrl, backgroundVoiceUrl, TTS/voice
 strings
 Native: libjingle_peerconnection_so.so (WebRTC), libexpo-av.so

Impact: The app holds microphone and camera permissions and ships a WebRTC stack ('libjingle_peerconnection_so.so') and voice/TTS surfaces, consistent with voice chat or calls with AI characters. Audio or video capture in an intimate-companion context is sensitive; if voice is sent to the Chinese backend identified in C1, this would compound into an Art. 9 and Art. 44 issue. Whether captured audio or video is transmitted to '*.xverse.cn' could not be confirmed by static analysis alone.

Impact Analysis

C1, C2, and C3 compound into a single pattern: an operator outside the EU, with no named EU representative or DPO (C3), routes personal data including intimate conversation content to Chinese infrastructure while denying any such transfer in its privacy policy (C1), and that intimate content is reachable by a child defeated only by a self-declared birthday field (C2). H1 through H3 and M1/M2 are the mechanics underneath that pattern: pre-consent SDK auto-init, insecure transport, a hardcoded credential, heavy ad/attribution tracking, and an unverified voice-capture pathway.

What ties all eight findings together procedurally is the correspondence record: eight 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: Eight Messages, Zero Replies, Zero Acknowledgments

Step 1 – Disclosure sent: RFI-IRFOS sends the full findings report on 30 June 2026 to saylo@xverse.cn and support@sayloai.com, BCC the Austrian Datenschutzbehoerde and the EDPS, stating an embargo date of 28 September 2026.

Step 2 through 7 – Six follow-ups, identical outcome: RFI-IRFOS sends further messages on 6 July, 17 July, 23 July, 31 July, 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 8 – Final follow-up: On 6 September 2026, RFI-IRFOS sends an eighth and final message, 68 days after the original disclosure. No further correspondence follows.

Step 9 – Embargo reached and passed: The embargo, stated once on 30 June 2026 and never revised, passes on 28 September 2026 with all eight findings unaddressed.

Step 10 – Publication: This report publishes 19 days after the embargo date. Across 68 days and eight messages sent to two functioning addresses, the correspondence record contains zero replies of any kind.

Data Protection – Article by Article

Art. 44, 46, 35, 13(1)(f), 14, 5(1)(a)/(2) GDPR – Third-country transfers, transfer impact assessment, and transparency: C1's undisclosed routing of login, chat, and LLM data to Chinese infrastructure directly contradicts the published privacy policy.

Art. 9, 8, 25, 35, 5(2), 44 GDPR – Special category data, child consent, data protection by design, DPIA, and third-country transfer: C2's intimate/romantic AI content is reachable by minors behind a trivially defeated age gate, and the content reaches a PRC LLM.

Art. 27, 37, 13(1)(a)/(b), 14 GDPR – EU representative, DPO, and transparency: C3's absence of any named controller, EU representative, or DPO blocks regulatory and data-subject recourse.

Art. 6(1), 7(1), 5(1)(a), 5(2) GDPR; ePrivacy Art. 5(3) – Lawfulness of processing and consent preceding storage/access: H1's pre-consent SDK auto-initialization.

Art. 32, 25 GDPR – Security of processing and data protection by design: H2's cleartext-permitting, user-CA-trusting production transport configuration.

Art. 32 GDPR – Security of processing: H3's hardcoded, apparently unrestricted API credentials.

Art. 6, 5(1)(c) GDPR; ePrivacy Art. 5(3) – Lawfulness and data minimisation: M1's ad-mediation and device-identifier harvesting.

Art. 5(1)(b)/(c), 6 GDPR; Art. 9 and 44 potentially applicable – M2's voice/video capture surface in an intimate-companion context.

Regulatory & Legal Landscape

X Original (Hong Kong) Limited and XVERSE Technology (Shenzhen, 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), 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). Given the German-locale targeting, competent German Landesdatenschutzbehörden and the EDPB cross-border cooperation channel may also be appropriate co-recipients at escalation.

Fine exposure under GDPR: Art. 83(5) applies to the Art. 44/46 transfer issue in C1, the Art. 9/8/35 special-category and minors issue in C2, and the Art. 27/37 accountability gap 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, and 5(1)(c) issues in H1, H2, H3, and M1, up to EUR 10,000,000 or 2% of total worldwide annual turnover. An operator with 5M+ installs that received eight written disclosures over 68 days and did not reply even once is itself a fact a regulator is likely to weigh alongside the eight technical findings.

Indicators of Compromise

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

```
C1 -- core-api.xverse.cn, prd-collect-llm.xverse.cn, asset-sh.xverse.cn, edgeone-prd-
    yunjing-proxy.xverse.cn
    sayloai.datasink.sensorsjourney.com/sa, beacon.qq.com, aegis.qq.com
    ad-host-backup-europe.oss-eu-central-1.aliyuncs.com

C2 -- CHAT_MODE_INTIMATE, isNsfw, setTeenModePassword (Hermes bundle strings)

C3 -- split_config.de.apk (de, de-DE locales); no Art. 27 rep, no DP0 in binary or
    privacy policy

H1 -- SensorsDataContentProvider, BigoAdsProvider, FacebookInitProvider auto-init at
    process start

H2 -- network_security_config.xml: cleartextTrafficPermitted="true", user CA trust in
    base-config

H3 -- google_api_key / google_crash_reporting_api_key / facebook_client_token in
    strings.xml (redacted above)

M1 -- AppLovin, Unity Ads, ironSource, Vungle, Pangle, Mintegral, BIGO, Tapjoy,
    Chartboost, AppsFlyer, Adjust

M2 -- RECORD_AUDIO, CAMERA permissions; libjingle_peerconnection_so.so (WebRTC)
```

Disclosure Timeline & Outcome

2026-06-30 Initial disclosure sent to saylo@xverse.cn and support@sayloai.com, BCC Austrian DSB and EDPS. Embargo stated as 2026-09-28. REF SAYLO-2026-R1-001.

2026-07-06, 2026-07-17, 2026-07-23, 2026-07-31, 2026-08-15, 2026-08-31 Six follow-up messages, each restating the eight 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 Eighth 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: eight RFI-IRFOS messages, zero replies.

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

Residual Risk & Recommendations

C1 – Immediate: disclose the Chinese processing chain in the privacy policy, document an Art. 46 transfer safeguard and transfer-impact assessment addressing the PRC National Intelligence Law and the Hong Kong National Security Law.

C2 – Immediate: replace the self-declared birthday/Teen Mode gate with a verified age-assurance mechanism in front of intimate/NSFW content, and document the Art. 35 DPIA for this special-category processing.

C3 – Immediate: designate a written Art. 27 EU representative and a DPO under Art. 37, and name the controller's legal entity and address in the privacy policy.

H1 – Near-term: gate all advertising/analytics SDK initialization, not only AdMob, behind a consent management platform.

H2 – Near-term: remove user-CA trust from the production base-config, disable global clear-text, and migrate the login/LLM API to TLS-only.

H3 – Near-term: rotate and restrict the Google/Firebase API key and the Facebook client token.

M1 – Near-term: remove or justify READ_PHONE_STATE/IMEI access and reduce the ad-mediation SDK footprint.

M2 – Near-term: document whether captured audio/video reaches '*.xverse.cn' and, if so, extend the C1 transfer safeguard to cover it.

Across all findings: establish a monitored intake path for security and data-protection disclosures sent to saylo@xverse.cn and support@sayloai.com that produces at minimum an acknowledgment, which eight 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 XVERSE, Tencent, Sensors Analytics, or Alibaba 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 SAYLO-2026-R1-001.