



Security & Privacy Disclosure, Final Report

WePlay (com.wejoy.weplay.us)

A voice party app ships a hardcoded analytics master key, 5,594 Tencent files, microphone access and a second PRC advertising SDK to every user. Five messages over 71 days drew no reply and no automated acknowledgment, and the report is published 16 days after the embargo.

PUBLIC DISCLOSURE, 17 OCTOBER 2026. EMBARGO REACHED 1 OCTOBER 2026, FIVE FINDINGS UNANSWERED

Target	WEJOY PTE. LTD., Singapore (UEN 202033872Z), WePlay
Package	com.wejoy.weplay.us v6.2.2
Platform analysed	Android, static analysis of the production APK installed from Google Play on a physical device on 2026-06-24
First report (R1)	2026-07-03 (REF RFI-2026-WJ-001)
Embargo date	2026-10-01
Report published	2026-10-17
Overall severity	CRITICAL
Findings	5 (3 Critical, 2 High)
Correspondence	5 messages over 71 days to support@wejoysg.com, 0 replies of any kind, 0 automated acknowledgments, 0 bounces
Authorities in copy	Austrian Data Protection Authority (DSB), European Data Protection Supervisor (EDPS)

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	Architecture & Data Flow	5
4	Correspondence Summary	5
5	Findings	6
5.1	C1: Hardcoded ThinkingData SECRETKEY constant in the production binary . .	6
5.2	C2: Full Tencent SDK footprint with RECORD_AUDIO on a social voice app, no age assurance found	7
5.3	C3: Pangle (ByteDance / TikTok) advertising SDK as a second independent PRC processor	8
5.4	H1: Hardcoded Firebase API key and Facebook application identifier	8
5.5	H2: No Article 27 EU representative designated	9
6	Impact Analysis	9
7	The Complete Chain	10
8	Data Protection, Article by Article	10
9	Regulatory & Legal Landscape	11
10	Indicators of Compromise & Reproducible Evidence	11
11	Disclosure Timeline & Outcome	11
12	Residual Risk & Recommendations	12

Executive Summary

WePlay is a social voice and party app operated by WEJOY PTE. LTD. in Singapore and distributed worldwide through Google Play. Version 6.2.2 contains a hardcoded SECRETKEY constant for the ThinkingData analytics platform, whose receiver endpoint is under PRC jurisdiction. It also contains 5,594 smali class files from the Tencent WeChat SDK, the RECORD_AUDIO permission, and the Pangle advertising SDK from ByteDance.

The governing thesis of this report is that a voice application with a plausibly young audience routes its dependency stack through two PRC-jurisdiction processors and gives users no visible age assurance and no EU point of contact. The evidence is static. It establishes what the binary contains and which permissions it requests. It does not establish which data leaves the device.

RFI-IRFOS disclosed five findings to WEJOY on 3 July 2026 with the Austrian DSB and the EDPS in copy. Four follow-ups followed on 23 July, 9 August, 31 August and 12 September. WEJOY did not answer any of the five messages and sent no automated acknowledgment. No address bounced. The embargo date of 1 October 2026 passed without a reply, and this report was published on 17 October 2026.

ID	Severity	Title
C1	CRITICAL	Hardcoded ThinkingData SECRETKEY constant in the production binary
C2	CRITICAL	Full Tencent SDK footprint with RECORD_AUDIO on a social voice app, no age assurance found
C3	CRITICAL	Pangle (ByteDance / TikTok) advertising SDK as a second independent PRC processor
H1	HIGH	Hardcoded Firebase API key and Facebook application identifier
H2	HIGH	No Article 27 EU representative designated

Subject & Operator Context

WePlay is published by WEJOY PTE. LTD., a company registered in Singapore under UEN 202033872Z. The app offers real-time voice rooms and party games and is distributed globally, including to users in the European Union. Singapore is a third country under GDPR Chapter V, so the operator falls under Art. 3(2) GDPR when it targets EU data subjects and must designate an Art. 27 representative. RFI-IRFOS found none (finding H2).

Architecture & Data Flow

The production APK is a native Android application. Static analysis shows three separate external stacks. First, the ThinkingData analytics SDK (package cn/thinkingdata/analytics/) with the receiver endpoint receiver.thinkingdata.cn. Second, the Tencent WeChat SDK (package com.tencent/, 5,594 smali files) with the Tencent infrastructure domains tencentci.cn and tencentcos.cn, together with the RECORD_AUDIO permission. Third, the Pangle advertising SDK (packages com/pangle/ and com/bytedance/pangle/). A Google API key and a Facebook application identifier sit in the resource files. All traffic uses HTTPS and the network security configuration disables cleartext traffic. The analysis did not include dynamic traffic capture, so the data actually sent to each destination is not documented here.

Correspondence Summary

RFI-IRFOS sent the first report on 3 July 2026 to support@wejoysg.com, the only contact address found for the operator, with the Austrian DSB and the EDPS in copy. The report asked for a response from the legal or privacy team and put three questions: whether the DPO is aware of the findings, whether an Art. 8 age assurance mechanism is documented, and whether WEJOY would address the findings before or after a supervisory authority contacts it. Follow-ups on 23 July, 9 August, 31 August and 12 September repeated the questions and asked at minimum for an acknowledgment of receipt. No reply of any kind arrived at any point. This is stated exactly as it occurred. The only address ever used was support@wejoysg.com, so it is possible that the messages never reached a privacy or legal function.

Findings

C1: Hardcoded ThinkingData SECRETKEY constant in the production binary

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9

```
.field public static final SECRETKEY:Ljava/lang/String;  
    = "[REDACTED IN PUBLIC REPORT, disclosed privately to WEJOY PTE. LTD. in R1]"  
  
# SDK receiver endpoint: receiver.thinkingdata.cn (PRC jurisdiction)
```

Limits of this finding. RFI-IRFOS analysed the binary statically and did not send any request to ThinkingData or WEJOY infrastructure. We did not test what the key authorises. R1 described the key as a master credential for the analytics data pipeline, based on the constant's name and the vendor's SDK structure. Whether the key permits read, export or event injection on the operator's ThinkingData project is a question for the operator and was one of the questions put to WEJOY.

Legal context. Analytics data processed through a PRC-headquartered provider falls under the PRC Data Security Law and the Personal Information Protection Law. The European Commission has issued no adequacy decision for the PRC, so a GDPR Chapter V transfer mechanism is required for personal data that reaches the provider. This is a legal assessment and not an established fact about this operator's contracts.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to CRITICAL because the constant sits in a binary distributed to every Google Play user worldwide, the receiving endpoint is under PRC jurisdiction, and the operator gave no response on whether the key is live.

Impact: The production APK of WePlay (com.wejoy.weplay.us v6.2.2) contains a hardcoded string constant named SECRETKEY in the class cn.thinkingdata.analytics.ThinkingAnalyticsSDK\$. The analytics SDK reports to receiver.thinkingdata.cn, an endpoint of a PRC-headquartered analytics provider. The constant is compiled into the DEX bytecode and is extractable by anyone who downloads the app from the Google Play Store.

C2: Full Tencent SDK footprint with RECORD_AUDIO on a social voice app, no age assurance found

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.0

```
smali class count, com/tencent/ namespace: 5594 files
hardcoded Tencent infrastructure domains: tencentci.cn, tencentcos.cn
AndroidManifest.xml: RECORD_AUDIO declared
```

Limits of this finding. The analysis is static. RFI-IRFOS did not capture runtime traffic and cannot state from this evidence which audio, if any, is transmitted to Tencent infrastructure. The finding establishes capability and plumbing: a complete Tencent communication stack, microphone permission, and Tencent storage and delivery domains inside one app.

Legal context. R1 argued that voice audio can permit unique identification and can therefore qualify as biometric data under Art. 9(1) GDPR when processed for that purpose. That is a legal interpretation and depends on the purpose of processing, which only the operator can state. Art. 8 GDPR requires verifiable parental consent for information society services offered directly to children below the age of digital consent. A real-time voice party app of this kind routinely attracts a significant under-18 audience. The privacy policy reviewed at the time of R1 did not name Tencent as a processor and did not address the PRC transfer or age assurance.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to CRITICAL because voice is the core feature of the product, the SDK footprint is the largest single component in the binary, and the app plausibly serves minors without a visible age assurance mechanism.

Impact: The binary contains 5,594 smali class files in the com/tencent/ namespace, which is the full Tencent WeChat communication stack and not a lightweight wrapper. The manifest declares RECORD_AUDIO. The binary hardcodes the Tencent infrastructure domains tencentci.cn and tencentcos.cn. RFI-IRFOS found no age verification or parental consent mechanism in this build.

C3: Pangle (ByteDance / TikTok) advertising SDK as a second independent PRC processor

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3

Pangle SDK present: com/pangle/, com/bytedance/pangle/
ByteDance HQ: Beijing, PRC
no adequacy decision for the PRC
no SCC reference in the privacy policy reviewed at R1

Limits of this finding. Static analysis shows the SDK is bundled. RFI-IRFOS did not observe which identifiers or events the SDK transmits at runtime.

Together with C1 and C2 this makes a second PRC-jurisdiction processor in the same app, so the transfer question applies to two independent recipients and not to one.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to CRITICAL because it is the second independent PRC processor inside one app that also requests microphone access and plausibly serves minors.

Impact: The binary embeds the Pangle advertising SDK (packages com/pangle/ and com/bytedance/pangle/). ByteDance is headquartered in Beijing, PRC. The privacy policy reviewed at the time of R1 did not name Pangle as a recipient and contained no reference to Standard Contractual Clauses for this processor.

H1: Hardcoded Firebase API key and Facebook application identifier

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, 6.9

```
google_api_key = [REDACTED IN PUBLIC REPORT, disclosed privately to WEJOY PTE. LTD.
in R1]
facebook_app_id = [REDACTED IN PUBLIC REPORT, disclosed privately to WEJOY PTE. LTD.
in R1]
```

Limits of this finding. Whether the Google API key carries API restrictions was not tested, and no request was sent to Google services with it. A Firebase key without restrictions can allow quota abuse or unwanted backend access, so the operator should confirm the restriction settings and the security rules of the associated project. A Facebook application identifier is a public identifier by design and is listed here because it shows a Facebook SDK integration that the privacy policy does not discuss.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the same binary also ships a PRC analytics credential (C1), so credential handling in this app deserves the same weight as the transfer questions.

Impact: The production APK contains a Google API key and a Facebook application identifier in cleartext resources. Both are extractable from any downloaded copy.

H2: No Article 27 EU representative designated

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:L, 6.9

This is an accountability gap and not a technical vulnerability, so the CVSS vector is a formal placeholder and the severity rests on the reasoning stated below. Art. 27 GDPR requires controllers and processors outside the EU that target EU data subjects to designate a representative in the Union. Without one, data subjects and supervisory authorities have no local point of contact. The Singapore Personal Data Protection Commission has no functioning email address that RFI-IRFOS could verify, so the supervisory channel for this operator is an open gap.

RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the missing representative removes the only local point of contact for EU data subjects in an app that combines microphone access, two PRC processors and a plausibly young audience.

Impact: WEJOY PTE. LTD. (Singapore, UEN 202033872Z) offers WePlay to users in the EU. RFI-IRFOS found no designated Art. 27 EU representative in any publicly accessible documentation, in the app or in the privacy policy reviewed at the time of R1.

Impact Analysis

The affected population is every user of WePlay, including EU residents and a significant number of minors who use voice party apps. The concrete consequences are these. Users speak in voice rooms through an SDK stack that includes a full Tencent communication library, and the privacy policy reviewed at the time of R1 did not name Tencent. Their device and usage data reaches an analytics provider and an advertising provider that are both subject to PRC law. A credential that appears to belong to the operator's analytics project is readable by anyone who downloads the app. And no EU representative exists whom an affected person or an authority could address.

The Complete Chain

A user, possibly a minor, installs WePlay from Google Play and joins a voice room. The app requests microphone access. The Tencent SDK stack is present in the binary together with Tencent storage and delivery domains. In parallel the ThinkingData SDK reports analytics events to receiver.thinkingdata.cn and the Pangle SDK serves and measures advertising through ByteDance. The privacy policy reviewed at R1 names neither Tencent nor Pangle and describes no age assurance. The same binary exposes the analytics SECRETKEY to anyone who unpacks it. When a researcher reports the combination, no one at the operator answers across five messages and 71 days. The chain ends at a user who cannot learn from the operator who receives their data, and at an authority that has no local representative to contact.

Data Protection, Article by Article

Article	Engaged by	Finding
Art. 3(2)	WePlay targets EU users from Singapore	H2
Art. 5(1)(a), (c)	Transparency and minimisation of a full Tencent SDK footprint and microphone access	C2
Art. 8	Services offered to children, no verifiable parental consent found	C2
Art. 9(1)	Voice as possible biometric data, depends on purpose, a legal interpretation	C2
Art. 13(1)(e)	Recipients not named in the privacy policy reviewed at R1	C2, C3
Art. 27	No EU representative designated	H2
Art. 28	Processor relationships with ThinkingData, Tencent and ByteDance not evidenced	C1, C2, C3
Art. 32(1)	Hardcoded credentials in a distributed binary	C1, H1
Art. 44-46	Transfers to PRC-jurisdiction recipients without adequacy decision or documented safeguard	C1, C2, C3

Regulatory & Legal Landscape

The competent authority for this case is the supervisory authority that receives the complaint of an affected EU data subject. RFI-IRFOS copied the Austrian Data Protection Authority (DSB) and the European Data Protection Supervisor (EDPS) on the first report and on three follow-ups. The operator is established in Singapore, where the Personal Data Protection Commission is the national regulator. RFI-IRFOS could not verify a working email address for that body, so this channel is an open gap. The PRC Data Security Law and the Personal Information Protection Law govern the three PRC-jurisdiction recipients.

Indicators of Compromise & Reproducible Evidence

```

package:                com.wejoy.weplay.us
version:                6.2.2
source:                Google Play, installed 2026-06-24 on a physical Android device
class:                Lcn/thinkingdata/analytics/ThinkingAnalyticsSDK$c (SECRETKEY
                    constant)
endpoint:                receiver.thinkingdata.cn
tencent namespace:      com/tencent/ (5594 smali files)
tencent domains:        tencentci.cn, tencentcos.cn
pangle namespaces:      com/pangle/, com/bytedance/pangle/
manifest permission:    RECORD_AUDIO
keys:                redacted in this public report, disclosed privately in R1
  
```

A second researcher can reproduce every item by unpacking the APK of the stated version with a standard decompiler and searching for the listed namespaces and the manifest entry.

Disclosure Timeline & Outcome

2026-06-24 Version 6.2.2 installed from Google Play on a physical device and analysed statically.

2026-07-03 R1 sent to support@wejoysg.com with the Austrian DSB and the EDPS in copy. Five findings, three questions. Embargo 2026-10-01. REF RFI-2026-WJ-001.

2026-07-23 First follow-up, 21 days, no reply of any kind, authorities in copy.

2026-08-09 Second follow-up, 37 days, no reply, authorities in copy.

2026-08-31 Third follow-up, 59 days, no reply, authorities in copy.

2026-09-12 Fourth follow-up, 71 days, no reply. Answer deadline 2026-09-19 passed without a response.

2026-10-01 Embargo date reached, as stated in R1 and in every follow-up, never revised. Correspondence status: five RFI-IRFOS messages, no reply of any kind, no automated acknowledgment, no bounce.

2026-10-17 This report published, 16 days after the embargo date.

Residual Risk & Recommendations

All five findings are open as of publication because WEJOY gave no response. RFI-IRFOS recommends that WEJOY rotate the ThinkingData SECRETKEY and move credentials out of the client binary, document the legal basis and transfer mechanism for each PRC-jurisdiction processor or remove the SDKs, implement and document age assurance and parental consent where minors can use voice rooms, restrict the Google API key and review the project security rules, and designate an Art. 27 representative. Users who are concerned about voice data in this app can withdraw microphone permission in Android settings. RFI-IRFOS will record any substantive reply from WEJOY next to the original findings in the public dataset, whenever it arrives.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings rest on static analysis of the published application with publicly available tools. No WEJOY, ThinkingData, Tencent or ByteDance servers, accounts or infrastructure were tested. Technical evidence is archived under chain of custody and is available to supervisory authorities on request. Research conducted under ISO/IEC 29147, the freedom of science (Art. 17 StGG) and GDPR Art. 89. REF RFI-2026-WJ-001.