Coordinated Privacy Disclosure, Final Report

Duolingo Android (com.duolingo)

Duolingo, Inc. (NASDAQ: DUOL), Pittsburgh, Pennsylvania, USA

AUTOMATED BOT DEFLECTION ONLY · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE EMBARGO, TWELVE MESSAGES, FIVE IDENTICAL AI-BOT REPLIES, ZERO HUMAN REPLY

Target	Duolingo, a language-learning Android app, also sold as a paid ad-free subscription
Package	com.duolingo
Operator	Duolingo, Inc. (NASDAQ: DUOL), Pittsburgh, Pennsylvania, USA
Initial Disclosure	2026-06-25
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six days after the embargo, an internal publishing gap, not a change in terms
Regulators	Austrian DSB, German BfDI (Duolingo's largest EU user cohort), CERT.at
Total Outbound Messages	12, across 71 days, all to privacy@duolingo.com, cc'ing the Austrian DSB and German BfDI.
Inbound Replies	5, all from privacy@duolingotest.zendesk.com, an automated AI support-desk agent ("Oscar"), each acknowledging the message without addressing any specific finding. No substantive human reply was ever received.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1 Executive Summary 4

2 Subject & Operator Analysis 5

3 Twelve Messages, Five Identical AI-Agent Replies, Zero Human Reply 5

4 Findings 6
- 4.1 C1: Google AdMob and Vungle/Liftoff Both Initialize Before Any Consent Screen 6
- 4.2 H1: Screenshot-Detection Monitoring Combined With Full Contact-Book Access in a Language-Learning App . . . 7
- 4.3 H2: Facebook Attribution and App Events Log Lesson Behavior and Purchases to Meta . . . 7
- 4.4 H3: Privacy Sandbox Attribution Permissions Active Alongside Pre-Consent AdMob Initialization . . . 8
- 4.5 M1: Adjust Attribution SDK Confirmed Active . . . 8
- 4.6 M2: Duplicate Boot-Time Auto-Start . . . 9

5 Data Protection, Article by Article 9

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to Duolingo, Inc. that its Android app, sold both as a free ad-supported tier and a paid ad-free subscription, initializes Google AdMob (initOrder=100) and Vungle/Liftoff (initOrder=102) as Android ContentProviders, both directBootAware, meaning both fire at process creation before any Activity and before any consent screen. Having an ad-supported tier is a disclosed product choice; the finding is the initialization order, ad-tracking infrastructure is already running by the time a user has seen any consent mechanism.

A second finding names a distinct, higher-severity gap: DETECT_SCREEN_CAPTURE, which notifies Duolingo in real time whenever a user screenshots the app with no documented language-learning feature requiring it, is declared alongside READ_CONTACTS and GET_ACCOUNTS, reading the device address book and account email addresses of people who have never used or consented to Duolingo. A separate finding names Meta's App Events and attribution tracking, logging lesson completions, streak data, paywall views, and purchases to a US processor for cross-app ad targeting, alongside an IntegrityManager module collecting device-level fraud-prevention signals.

Twelve messages were sent to privacy@duolingo.com across 71 days, cc'ing the Austrian DSB and German BfDI, Duolingo's largest EU user cohort's supervisory authority. Five drew a reply, every one of them from privacy@duolingotest.zendesk.com, an automated AI support-desk agent identified in its own replies as "Oscar," each acknowledging receipt without addressing a single specific finding. Not one substantive, human-authored reply was ever received. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Duolingo Android application (com.duolingo, version 6.85.7, 136.9 MB), as reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Duolingo's, Google's, Vungle's, or Meta's backend infrastructure was performed.

Disposition

Six findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. Screenshot-detection monitoring combined with full-contact-book access in a language-learning app reaches HIGH on the computed CVSS score alone. Pre-consent AdMob and Vungle/Liftoff initialization, active Facebook attribution and app-events tracking, and undisclosed Privacy Sandbox attribution permissions all correct to MEDIUM, as does an Adjust attribution SDK integration. Boot-time auto-start corrects to OBSERVATIONAL. Twelve messages were sent across 71 days, five drawing an identical automated AI-agent acknowledgment; not one substantive human reply was ever received.

ID	Severity	Title
C1	MEDIUM	Google AdMob and Vungle/Liftoff Both Initialize Before Any Consent Screen

ID	Severity	Title
H1	HIGH	Screenshot-Detection Monitoring Combined With Full Contact-Book Access in a Language-Learning App
H2	MEDIUM	Facebook Attribution and App Events Log Lesson Behavior and Purchases to Meta
H3	MEDIUM	Privacy Sandbox Attribution Permissions Active Alongside Pre-Consent AdMob Initialization
M1	MEDIUM	Adjust Attribution SDK Confirmed Active
M2	OBSERVATIONAL	Duplicate Boot-Time Auto-Start

Subject & Operator Analysis

Duolingo is a language-learning platform operated by Duolingo, Inc. (NASDAQ: DUOL), sold both as a free ad-supported product and as a paid ad-free subscription.

Several genuine positives are worth naming. allowBackup is correctly set to false, keeping learning progress out of unencrypted cloud backup. usesCleartextTraffic defaults correctly to false. A network security configuration is present. Biometric login is correctly implemented. The Vungle SDK's own getCollectConsent method indicates a consent-collection hook already exists in the architecture; the fix for C1 is wiring that hook ahead of ContentProvider initialization, not building new infrastructure.

Twelve Messages, Five Identical AI-Agent Replies, Zero Human Reply

This case's correspondence record involved a working contact channel from the first message; no address bounced. Twelve messages were sent to privacy@duolingo.com across 71 days, cc'ing the Austrian DSB and the German BfDI, the supervisory authority for Duolingo's largest EU user cohort. Five of the twelve drew a reply, every one of them from privacy@duolingotest.zendesk.com, an automated AI support-desk agent that identifies itself as "Oscar" in its own replies, each acknowledging the message generically without addressing any specific finding or answering the three yes/no questions posed in the original disclosure. Not one substantive, human-authored reply was ever received.

Findings

C1: Google AdMob and Vungle/Liftoff Both Initialize Before Any Consent Screen

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.

Both MobileAdsInitProvider (Google AdMob, initOrder=100) and VungleProvider (initOrder=102) are declared directBootAware="true", meaning both fire at process creation, before any Activity and therefore before any consent dialog; Vungle fires before AdMob since a higher initOrder runs first. The Vungle SDK includes a getCollectConsent method, indicating a consent-collection hook already exists in the architecture, it simply does not wrap the ContentProvider initialization it needs to gate.

```
com.google.android.gms.ads.MobileAdsInitProvider   initOrder=0x64 (100),
    directBootAware=true
com.vungle.ads.VungleProvider                      initOrder=0x66 (102),
    directBootAware=true
```

Impact: Two ad-network trackers begin running before a user has seen a single consent notice, even though a paid, ad-free subscription tier exists.

Fix: Wrap both providers' initialization behind the existing consent-collection hook (the Vungle getCollectConsent method already present) so it runs before, not after, ContentProvider initialization. No confirmation that this has occurred was ever received.

H1: Screenshot-Detection Monitoring Combined With Full Contact-Book Access in a Language-Learning App

HIGH, 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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

DETECT_SCREEN_CAPTURE notifies Duolingo in real time whenever a user takes a screenshot, with no documented user-facing language-learning feature requiring it. READ_CONTACTS and GET_ACCOUNTS are declared alongside it, reading the device address book and linked account email addresses, including contacts of third parties who have never used or consented to Duolingo.

```
android.permission.DETECT_SCREEN_CAPTURE
android.permission.READ_CONTACTS
android.permission.GET_ACCOUNTS
```

Impact: A user's screenshot activity is monitored with no disclosed purpose, and the personal data of non-users, people in the device's contact list who never agreed to anything, is read and potentially processed.

Fix: Disclose the screen-capture detection use case explicitly or remove it, and gate contact access behind an explicit, narrowly scoped friend-finding flow that does not read the full address book by default. No confirmation that this has occurred was ever received.

H2: Facebook Attribution and App Events Log Lesson Behavior and Purchases to Meta

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.

Facebook App Events and attribution tracking are active, logging lesson completions, streak data, paywall views, and in-app purchases to Meta for cross-app ad targeting and lookalike audience modeling. An IntegrityManager module collects device-level signals for Meta's fraud-prevention stack. Meta is a US company subject to the CLOUD Act.

```
com.facebook.sdk.attributionTracking (active)
com.facebook.sdk.appEventPreferences
com.facebook.appevents.integrity.IntegrityManager
```

Impact: Detailed learning-behavior and purchase data is forwarded to a US-based advertising processor for cross-app targeting, with device-level fraud-prevention signals collected alongside it.

Fix: Name Meta explicitly as a processor under Art. 28 and Art. 13(1)(e), and gate App Events behind consent. No confirmation that this has occurred was ever received.

H3: Privacy Sandbox Attribution Permissions Active Alongside Pre-Consent AdMob Initialization

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.

AD_ID, ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, and ACCESS_ADSERVICES_TOPICS are all active with no confirmed consent-management-platform gate, compounding the pre-consent AdMob initialization documented in C1.

```
com.google.android.gms.permission.AD_ID
android.permission.ACCESS_ADSERVICES_AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_TOPICS
```

Impact: Cross-app behavioral attribution and advertising-identifier collection compound the pre-consent ad-network initialization already documented, without a confirmed consent gate covering either.

Fix: Confirm and document the CMP's coverage of all four AdServices permissions. No confirmation that this has occurred was ever received.

M1: Adjust Attribution SDK Confirmed Active

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.

Adjust's attribution SDK is confirmed active via AdjustPreinstallReferrerReceiver. IMEI fingerprinting modules were not confirmed in this static scan and were held for a deeper follow-up review that never took place, given the absence of any engagement.

```
AdjustPreinstallReferrerReceiver (confirmed active)
```

Impact: Install and purchase attribution is tracked through a third-party processor alongside the app's own ad-network integrations.

Fix: Document the Adjust integration under Art. 28 and Art. 13(1)(e). No confirmation that this has occurred was ever received.

M2: Duplicate Boot-Time Auto-Start

OBSERVATIONAL — not independently CVSS-scored; auto-start alone carries no direct confidentiality, integrity, or availability impact to score.

BOOT_COMPLETED is declared twice in the manifest, meaning the app starts automatically at device boot.

Impact: The app begins running at every device boot without an explicit user launch, a transparency point, not a demonstrated technical exposure on its own.

Fix: Document the purpose of boot-time auto-start, or remove the duplicate declaration if not load-bearing. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 7, Art. 25	C1	Pre-consent ad-network ContentProvider initialization.
Art. 5(1)(b)/(c), Art. 6(1)	H1	Undisclosed screenshot monitoring and full contact-book access.
Art. 13(1)(e), Art. 28, Art. 6(1)	H2	Undisclosed behavioral and purchase data forwarded to Meta.
Art. 5(1)(b), Art. 6(1)	H3	Undisclosed cross-app attribution tracking without a confirmed consent gate.
Art. 28, Art. 13(1)(e)	M1	Undisclosed third-party attribution processor.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, H1 reaches HIGH on its computed CVSS v4.0 score alone, no editorial escalation applied; C1, H2, H3, and M1 correct to MEDIUM to match their own

computed bands; M2 is classified OBSERVATIONAL because auto-start alone carries no direct scoreable impact. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: DUOLINGO-2026-R1.