Coordinated Security & Privacy Disclosure, Final Report

Disneyland Android App (com.disney.wdpro.dlr, v8.22)

Nine written notices, ninety days, one bounced regulator address, zero replies of any kind

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FOUR FINDINGS UNADDRESSED AFTER NINE NOTICES

Target	The Walt Disney Company / Disneyland Paris
Product audited	Disneyland Android App, com.disney.wdpro.dlr, v8.22
Disclosure reference	REF DISNEYLANDEU-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 Memory Maker facial recognition of children absent explicit Art. 9(2)(a) consent, CVSS v4.0 8.8, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Disneyland Android application and identified three CRITICAL and one HIGH finding: a Firebase project key hardcoded in the shipped APK exposing the Mobile Disney Experience (MDX) platform's remote configuration, park capacity parameters, and pricing experiments, a Memory Maker/PhotoPass facial-recognition feature enrolling and matching children's faces across an entire park venue absent explicit Art. 9(2)(a) consent and implicating the EU AI Act's Art. 5(1)(d) prohibition on real-time biometric identification in publicly accessible spaces, a MagicBand RFID wristband producing a persistent, undisclosed-retention location log of every ride, restaurant, and restroom visit by children throughout the park, and a manifest declaration of usesCleartextTraffic="true" that directly contradicts the app's own Network Security Configuration, which declares cleartextTrafficPermitted="false".

Across nine written notices over ninety days, spanning two parallel Gmail threads that appear to be an artifact of the same duplicate-tracking defect class noted elsewhere in RFI-IRFOS's outreach system rather than two distinct cases, no acknowledgment, dispute, or substantive reply of any kind was ever received from Disney or The Walt Disney Company specifically on this case. The only inbound message on either thread was an automated delivery-failure bounce for the bcc'd French CNIL address, which was never corrected or resent. None of RFI-IRFOS's five standing questions, on Art. 9(2)(a) and Art. 35 coverage for Memory Maker, the EU AI Act Art. 5(1)(d) basis for continued operation, MagicBand's retention and sharing policy, the Firebase/cleartext remediation timeline, or Art. 33 notification, ever received an answer.

Scope: Static analysis of the publicly downloaded production Disneyland Android APK (v8.22), on an authorized test device, only. No Disney account, backend, park infrastructure, or on-site systems were accessed or tested.

Disposition

R1 sent 21 June 2026 to privacy@disney.com, guest.services@disneystore.com, Disney.Parks.News@disney.com, and TWDC.Advertising.EMEA@disney.com, bcc the French CNIL (bounced, address invalid, never resent), the Austrian Datenschutzbehoerde, and CERT.at. Across nine written notices spanning two parallel Gmail threads for the same underlying finding set, no acknowledgment, dispute, or substantive reply of any kind was ever received from Disney or The Walt Disney Company on this case.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the production APK
C2	CRITICAL	Memory Maker facial recognition of children absent explicit Art. 9(2)(a) consent
H1	HIGH	MagicBand RFID real-time location tracking of children
C3	CRITICAL	Manifest and Network Security Configuration conflict on cleartext traffic

Subject & Operator Analysis

Disneyland Paris operates under EU jurisdiction as part of The Walt Disney Company. Correspondence in this case was addressed to Disney's global privacy team and Disneyland Paris guest-services and advertising contacts, no verbatim legal-entity name was returned in any reply, as none was ever received.

Findings

C1: Firebase API key hardcoded in the production APK

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

Firebase key AIzaSyDrwI4nI6odp8LMBKBAG7IpkQe2YYhZ8Us, project mdxdlr420584321649 (the identifier decodes to Mobile Disney Experience + Disneyland Resort), App ID 1:420584321649:android:088841cbe21603f37021d0, storage bucket mdxdlr420584321649.appspot.com, are hardcoded in the shipped APK.

With this key, an external party can probe the MDX platform Firebase project, read remote configuration values including park capacity parameters, attraction wait-time algorithms, A/B test parameters, and pricing experiments, and access Firebase Storage. No reply of any kind addressed this finding.

Impact: Operational and commercial configuration data for the park platform is exposed to any party extracting the key from the public APK.

Fix: Rotate the exposed key, confirm remote-config and storage access rules are deny-by-default, and enforce App Check for this project.

C2: Memory Maker facial recognition of children absent explicit Art. 9(2)(a) consent

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.8

Memory Maker/PhotoPass smali (2,991 classes) and an active camera integration (chassis_camera) confirmed within the Disney Parks Experience Platform (DPEP) core layer enroll a guest's face on park entry and match it against every photographer's capture across the entire venue.

This is framed under GDPR Art. 9(1)/9(2)(a) (special-category biometric data) and Art. 8 (children's data), and separately implicates the EU AI Act's Art. 5(1)(d) prohibition on real-time biometric identification in publicly accessible spaces, whose compliance deadline passed during this case's correspondence. CNIL deliberation 2019-114 is cited as relevant precedent. No reply of any kind addressed this finding.

Impact: Children's biometric data may be enrolled and matched park-wide without the explicit, verifiable parental consent Art. 9(2)(a) requires, in a practice the EU AI Act separately prohibits in publicly accessible spaces.

Fix: Suspend park-wide facial matching pending a documented Art. 35 DPIA and explicit, verifiable Art. 9(2)(a) consent, and confirm the feature's compatibility with EU AI Act Art. 5(1)(d).

H1: MagicBand RFID real-time location tracking of children

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

MagicBand integration (1,815 smali classes) performs real-time RFID location tracking of children via a body-worn wristband throughout the theme park, producing a persistent location log of every ride, restaurant, and restroom visit.

Retention period and any onward sharing of this location log are undisclosed. No reply of any kind addressed this finding.

Impact: A persistent, granular location history of children's movements through a theme park is generated with no disclosed retention or sharing policy.

Fix: Publish a defined retention period for MagicBand location logs and disclose any onward sharing explicitly.

C3: Manifest and Network Security Configuration conflict on cleartext traffic

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

The manifest declares usesCleartextTraffic="true" while the app's own Network Security Configuration separately declares cleartextTrafficPermitted="false" – a direct configuration conflict.

Whichever declaration the runtime actually honors, the presence of a manifest-level cleartext allowance on a park app handling guest and payment-adjacent data is a hardening failure in its own right. No reply of any kind addressed this finding.

Impact: Traffic may be transmitted in cleartext on some code paths despite the app's own network security policy declaring cleartext prohibited.

Fix: Remove the manifest's usesCleartextTraffic override so it does not contradict the Network Security Configuration, and confirm no traffic path relies on cleartext.

Nine Notices, Two Threads, One Bounce, Zero Replies

This case's nine written notices were sent across two parallel Gmail threads carrying the same finding set, an artifact of the same thread-duplication pattern noted elsewhere in RFI-IRFOS's outreach system rather than two genuinely distinct cases. Across both threads and ninety days, no acknowledgment, dispute, or substantive reply of any kind was ever received from Disney or The Walt Disney Company on this case specifically. The only inbound message was an automated delivery-failure bounce for the bcc'd French CNIL address, which was never corrected or resent during the case.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded Firebase key exposing platform configuration
C2	GDPR Art. 8, Art. 9, Art. 35; EU AI Act Art. 5(1)(d)	Park-wide facial recognition of children absent explicit consent
H1	GDPR Art. 5(1)(b), Art. 8, Art. 13	Undisclosed retention of children's RFID location logs
C3	GDPR Art. 32(1)(a)	Manifest/Network Security Configuration conflict on cleartext traffic

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to four Disney addresses; bcc CNIL bounces immediately, Austrian DSB and CERT.at also bcc'd; C1 and C2 findings; a EUR 75,000 NDA research-engagement figure was offered under the R1 policy then in force – historical record only, not a currently open offer
2026-06-28	Parallel follow-up on the privacy@disney.com-only thread adds finding H1 (MagicBand)
2026-07-27	Follow-up flags the EU AI Act's August 2026 biometric-identification prohibition deadline approaching
2026-08-15	Follow-up notes the EU AI Act deadline has now passed with Memory Maker's status unaddressed
2026-08-24	Follow-up invokes the Art. 33(4) GDPR 72-hour notification clock
2026-09-04	Follow-up on the four-address thread restates the case; a EUR 250,000 full-donation figure was referenced under the same then-current policy – also historical only
2026-09-12	Follow-up adds finding C3 (manifest/NSC cleartext conflict), sets a three-questions deadline of 18 September, discloses weekly APK re-pull/diff during the embargo
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Suspend Memory Maker's park-wide facial matching pending a documented Art. 35 DPIA and confirmation of EU AI Act Art. 5(1)(d) compatibility.
- Publish a defined retention and sharing policy for MagicBand location logs.
- Remove the manifest's cleartext-traffic override so it no longer contradicts the app's own Network Security Configuration.
- Rotate the exposed Firebase key and confirm deny-by-default access rules with App Check enforced.
- Correct the bounced French CNIL notification address and confirm the regulator has actually received this disclosure.

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 Coordinated disclosure per ISO/IEC 29147. GDPR Art. 5, 8, 9, 13, 25, 32, 33, 35. EU AI Act Art. 5(1)(d). REF DISNEYLANDEU-2026-R1.