Coordinated Security & Privacy Disclosure, Final Report

Airbnb for Android (com.airbnb.android)

Global accommodation marketplace, misrouted to personal-safety support twice

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, MISROUTED TO SUPPORT TWICE, NEVER REACHED PRIVACY OR SECURITY

Target	Airbnb Ireland UC, 8 Hanover Quay, Dublin 2, Ireland / Airbnb, Inc., San Francisco, California, US
Product audited	Airbnb for Android, com.airbnb.android, v26.25.1
Disclosure reference	REF AIRBNB-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C2 cleartext biometric routing to China, CVSS v4.0 8.6 High) / H1 host location fingerprinting scores 8.7 High

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Airbnb Android application and identified seven findings, two CRITICAL, five HIGH. The most significant: identity verification photographs, GDPR Art. 9 biometric data, are routed to api.faceid.com, operated by a Chinese facial recognition company, over a network security configuration that explicitly permits cleartext HTTP for that exact domain, alongside cleartext exceptions for China Mobile and China Unicom single sign-on endpoints and a Baidu CDN domain.

Separately, four Firebase API keys are hardcoded in the production binary, including one pointing to a project named airbedandbreakfast-com, the company's own pre-2009 founding name, suggesting a credential in continuous production use for an estimated eight to ten years, the longest credential age RFI-IRFOS has documented across its full research series. Incognia, a US location-identity vendor, builds an indoor spatial fingerprint of where Airbnb hosts physically live, more precise than GPS, while FingerprintJS maintains a persistent device identity that survives app reinstallation and factory reset.

Fifteen written notices were sent over 91 days. privacy@airbnb.com bounced on every attempt from day one. Two of the human replies received, from Airbnb's Community Support and Urgent Support teams, treated the disclosure as an in-app personal safety complaint rather than a GDPR notification, the second explicitly asking what happened that made the sender feel unsafe during a reservation. No privacy, legal, or security contact ever substantively engaged with any of the seven findings.

Scope: Static analysis of the publicly downloaded production Airbnb Android APK, on an authorized test device, only. No Airbnb backend, account, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to Airbnb's HackerOne-adjacent security channel, bcc the Austrian DSB, CERT.at, and the Irish DPC as Airbnb Ireland UC's lead supervisory authority. privacy@airbnb.com bounced on every attempt from 20 June 2026 onward. Fifteen written notices followed. Two of the replies received, on 17 August and 12 September 2026, came from Airbnb's Community Support and Urgent Support teams respectively, each treating a coordinated GDPR disclosure as a personal in-app safety complaint, the second asking what happened that made the sender feel unsafe during a reservation. Neither a privacy, legal, nor security contact ever substantively engaged.

ID	Severity	Title
C1	CRITICAL	Four hardcoded Firebase keys, one pointing to a project named after the company's pre-2009 founding name
C2	CRITICAL	Cleartext HTTP permitted for biometric identity verification to a Chinese facial recognition API
H1	HIGH	Incognia: indoor location fingerprinting builds a spatial model of where hosts live

ID	Severity	Title
H2	HIGH	FingerprintJS: persistent device identity surviving re-installation and factory reset
H3	HIGH	Tencent and Alipay SDKs present in the global EU-distributed binary
H4	HIGH	Singular: advertising exposure correlated directly with booking history
H5	HIGH	POST_PROMOTED_NOTIFICATIONS with no disclosed consent basis at onboarding

Subject & Operator Analysis

Airbnb Ireland UC (8 Hanover Quay, Dublin 2) is the EU controller entity, making Ireland's Data Protection Commission the lead supervisory authority; Airbnb, Inc. (San Francisco, California) is the global parent. Airbnb operates a HackerOne vulnerability disclosure programme, which RFI-IRFOS's original notice referenced but did not route through, since this disclosure concerns GDPR compliance findings rather than exploitable security vulnerabilities in the bounty programme's scope.

Positive Observations

- TLS is correctly enforced for airbnb.com, airbnbchina.cn, and airbnb.cn, the platform's core domains.
- NFC for smart-lock self-check-in is legitimate and well-scoped to its stated purpose.
- No FullStory or session-replay SDK was found (zero references).
- targetSdk 35 (Android 15) is near-current.
- A diversified, non-monopolized payment SDK stack (Braintree, Stripe, Adyen, Klarna, Worldline) was found, rather than a single vendor holding exclusive payment-data access.

Findings

C1: Four hardcoded Firebase keys, one pointing to a project named after the company's pre-2009 founding name

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

Four distinct Firebase API keys are hardcoded in the production APK, pointing to two separate Firebase databases: airbedandbreakfast-com-api-project-622686756548.firebaseio.com and airbnb-38fb0.firebaseio.com.

```
AIzaSyCuXVjANn4sJalYV42BLA4xr9ntx_9V67o
AIzaSyDgg0j0epSBWrcvz0G6jzp9oVsi9WvRnrk
AIzaSyDOfRrQ5Pa4_0SiY7S_g5YFIX24pWXKngA
AIzaSyCPS5GasxhHtX-e8EI755dvl8U_CR_3R6o

airbedandbreakfast-com-api-project-622686756548.firebaseio.com
airbnb-38fb0.firebaseio.com
```

No response was received naming this finding. airbedandbreakfast.com was Airbnb's own name before its 2009 rebrand. A Firebase project still carrying that founding-era name suggests the credential has been in continuous production use for approximately eight to ten years without rotation, the longest credential age RFI-IRFOS has documented in its research series to date.

Impact: Four separate exposed credentials, one with an estimated decade of unrotated production use, enable FCM probing and potential further backend access.

Fix: Rotate all four keys, restrict each to the production certificate fingerprint, and audit whether the airbedandbreakfast-com legacy project is still in active use at all.

C2: Cleartext HTTP permitted for biometric identity verification to a Chinese facial recognition API

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 network security configuration explicitly permits cleartext HTTP traffic for api.faceid.com (Beijing Jieyi Technology Co., Ltd., a Chinese cloud facial-recognition provider actively referenced in Airbnb's identity-verification code), alongside cleartext exceptions for cmpassport.com (China Mobile SSO), 10010.com (China Unicom), and bdimg.com (Baidu CDN).

```
<domain-config cleartextTrafficPermitted="true">
    <domain includeSubdomains="true">api.faceid.com</domain>
    <domain includeSubdomains="true">cmpassport.com</domain>  <!-- China Mobile SSO
    -->
    <domain includeSubdomains="true">10010.com</domain>       <!-- China Unicom -->
    <domain includeSubdomains="true">bdimg.com</domain>       <!-- Baidu CDN -->
</domain-config>
```

No response was received naming this finding. Facial photographs submitted for identity verification are biometric data under GDPR Art. 9(1). Transmitting that data over cleartext HTTP is a direct Art. 32(1)(a) failure independent of the recipient; that the recipient is also a China-based processor with no EU adequacy decision under Art. 44 compounds it. Three independent GDPR concerns sit on a single HTTP call.

Impact: Biometric identity-verification photographs can be intercepted or modified in transit by anyone on the same network, hotel WiFi and airport networks being the most immediately relevant threat model for a travel app, before ever reaching a jurisdiction with no EU adequacy decision.

Fix: Remove the cleartext exception for api.faceid.com and enforce TLS for all identity-verification traffic; separately, assess and disclose the Art. 44 transfer basis for routing biometric data to a Chinese processor at all.

H1: Incognia: indoor location fingerprinting builds a spatial model of where hosts live

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

Incognia (Palo Alto, California), 2,175 classes, continuously samples WiFi, Bluetooth, sensor, and GPS data to build a habitual location fingerprint, marketed by the vendor as 'location identity' and 'home address verification.'

No response was received naming this finding. For hosts, this builds an indoor spatial model of their home more precise than GPS alone; for guests, it functions as a continuous location profile used as a fraud signal. This is a US company processing intimate location data with no EU adequacy decision applicable to the transfer.

Impact: Airbnb hosts, who use the app as a livelihood tool rather than an optional consumer choice, have an indoor model of their own home built by a third-party US vendor as a background function of hosting.

Fix: Scope Incognia's sampling to the minimum needed for its stated fraud-prevention purpose, disclose it specifically to hosts as distinct from guests, and publish the applicable Art. 44-49 transfer mechanism.

H2: FingerprintJS: persistent device identity surviving reinstallation and factory reset

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

Fingerprint Inc. (Chicago, US), 877 classes, creates a hardware and software fingerprint that persists across app reinstallation, advertising ID reset, and, via server-side re-association, factory reset.

No response was received naming this finding. Combined with Incognia (H1), Airbnb operates a dual persistent identity layer, device and location, that ordinary user actions like resetting an advertising ID or performing a factory reset cannot clear.

Impact: Users cannot meaningfully reset their tracked identity on the platform through any standard device-level privacy action.

Fix: Provide a genuine, working reset mechanism for the FingerprintJS-derived identity, independent of device-level resets that the SDK is specifically designed to survive.

H3: Tencent and Alipay SDKs present in the global EU-distributed binary

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

Tencent (189 classes) and Alipay (48 classes) SDKs are both present in the same binary distributed to EU users, rather than scoped to a China-specific build variant.

No response was received naming this finding. RFI-IRFOS recommends the same build-flavor separation here that it has recommended to other travel platforms carrying China-market payment and social SDKs: a distinct China-market APK versus a global APK, so EU users are not shipped code paths for services with no relevance or applicable legal basis in their jurisdiction.

Impact: EU users receive a binary containing Chinese payment and social SDK code with no apparent EU-market function, an unnecessary attack surface and transfer-risk expansion.

Fix: Separate the China-market and global builds so EU-distributed APKs do not carry Tencent or Alipay SDK code.

H4: Singular: advertising exposure correlated directly with booking history

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

Singular Labs (San Francisco, US), 182 classes, correlates which advertisements a user saw with which bookings they subsequently made.

No response was received naming this finding. This links ad-response behavior directly to travel and accommodation choices, a data flow that reveals meaningful information about a user's movements and financial decisions to a third-party US attribution vendor.

Impact: A user's travel and accommodation decisions are linked to their advertising exposure history by a third-party vendor with no disclosed specific consent basis.

Fix: Disclose Singular as a data recipient under Art. 13(1)(e) and confirm the Art. 6 basis for this specific correlation.

H5: POST_PROMOTED_NOTIFICATIONS with no disclosed consent basis at onboarding

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

android.permission.POST_PROMOTED_NOTIFICATIONS, distinct from ordinary service notifications, enables sending advertising-category push notifications. No consent basis for promotional notifications specifically was observed at onboarding.

No response was received naming this finding.

Impact: Users may receive advertising-category notifications with no specific consent step distinct from general service notification consent.

Fix: Add a distinct, specific consent step for promotional notifications, separate from service notifications, at onboarding.

Date	Event

Disclosure Timeline & Outcome: Two Personal-Safety Misroutes, Never a Privacy Contact

Date	Event
2026-06-20	R1 sent, referencing Airbnb's HackerOne programme without routing through it, bcc Austrian DSB/CERT.at/Irish DPC
2026-06-27	press+noreply@airbnb.com auto-acknowledges; no substantive reply
2026-07-04 / 07-17 / 07-27	Follow-ups, no substantive reply
2026-07-27	privacy@airbnb.com confirmed bouncing on every attempt since 20 June; corrected address sought
2026-07-29	Airbnb's general support inbox (reply@email-support.airbnb.com) responds and closes the thread as a duplicate support case
2026-08-05	Follow-up sent directly to dpo@airbnb.com after the routing failure
2026-08-15	Stated deadline passes with no substantive reply
2026-08-17	'Jenna R' from Airbnb replies: 'Thank you for bringing this issue to our attention. We're currently investigating your case', treating the GDPR disclosure as a generic support ticket
2026-09-04	66-day follow-up, no substantive reply
2026-09-12	84-day follow-up; same day, 'Rachelle' from Airbnb's Urgent Support team replies asking what happened that made the sender 'feel unsafe during reservation,' treating a coordinated GDPR disclosure as an in-app personal safety complaint
2026-09-19	Embargo closes; this report publishes

Fifteen written notices across 91 days produced exactly two substantive-sounding human replies, both from Airbnb's consumer support organization rather than any privacy, legal, or security function, and both fundamentally misreading the nature of the correspondence: the

first as a generic support case under investigation, the second as an in-app personal safety incident requiring the sender to describe what made them feel unsafe. Neither reply engaged with a single one of the seven technical findings. All seven stand exactly as originally reported.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b)	Near-decade-old credential, longest in RFI-IRFOS's research series
C2	GDPR Art. 9(1), Art. 32(1)(a), Art. 44	Cleartext biometric data routed to a Chinese processor
H1	GDPR Art. 5(1)(b), Art. 13(1)(e)(f), Art. 44	Indoor location fingerprinting of hosts' homes
H2	GDPR Art. 5(1)(c), Art. 13, Art. 25(1)	Persistent identity surviving standard user resets
H3	GDPR Art. 13(1)(e)(f), Art. 44	China-market SDKs in the global EU binary
H4	GDPR Art. 5(1)(b), Art. 13(1)(e)(f), Art. 44	Ad exposure correlated with booking history
H5	GDPR Art. 6(1); ePrivacy	Undisclosed consent basis for promotional notifications

Residual Risk & Recommendations

- Remove the cleartext exception for api.faceid.com immediately; this is the single highest-priority item given the biometric data category involved.
- Rotate all four exposed Firebase credentials, with priority on the decade-old airbedandbreakfast-com project.
- Scope and disclose Incognia's indoor location fingerprinting specifically to hosts.
- Provide a genuine reset mechanism for the FingerprintJS persistent identity.
- Separate China-market and global APK builds.
- Disclose Singular as a data recipient and confirm its legal basis.
- Add a specific consent step for promotional notifications.
- Establish an actual routing path from a GDPR disclosure to Airbnb's privacy, legal, or security function; consumer support and Urgent Support routing this correspondence as a generic ticket and a personal-safety complaint respectively is itself an intake-process failure independent of the seven technical findings.

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. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 9, 13, 25, 32, 44-49. REF AIRBNB-2026-R1.