Coordinated Security & Privacy Disclosure, Final Report

Booking.com for Android (com.booking, v32.7.102)

Thirteen written notices, ninety-one days, one non-automated reply that redirected to a bug-bounty programme, zero substantive answers

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SEVEN FINDINGS UNADDRESSED AFTER THIRTEEN NOTICES

Target	Booking.com B.V., Amsterdam, Netherlands, a subsidiary of Booking Holdings Inc. (NASDAQ: BKNG)
Product audited	Booking.com for Android, com.booking, v32.7.102
Disclosure reference	REF BOOKING-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C3 WeChat/Tencent SDK routing EU user data to Chinese infrastructure with no Art. 44 transfer mechanism disclosed, CVSS v4.0 8.7, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Findings 4
- 3.1 C1: Firebase/OAuth API key hardcoded in the production APK 4
- 3.2 C2: Zero certificate pinning across all payment and reservation traffic 5
- 3.3 C3: WeChat/Tencent SDK (181 classes) in the global APK – EU user data routed to Chinese infrastructure 5
- 3.4 H1: RECORD_AUDIO permission with no identifiable implementation 6
- 3.5 H2: targetSdkVersion 31 (Android 12) in 2026 6
- 3.6 H3: GET_ACCOUNTS, MANAGE_ACCOUNTS, and AUTHENTICATE_ACCOUNTS declared together 7
- 3.7 H4: READ_CALENDAR and HIGH_SAMPLING_RATE_SENSORS – scope beyond booking 7

4 One Reply in Ninety-One Days, and It Was a Redirect 8

5 Data Protection, Article by Article 8

6 Disclosure Timeline & Outcome 9

7 Residual Risk & Recommendations 10

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Booking.com Android application and identified three CRITICAL and four HIGH findings: a Firebase/OAuth API key hardcoded in the shipped APK, zero certificate pinning across all payment and reservation traffic on an application handling Braintree, PayPal, and Venmo payment SDKs, a 181-class WeChat/Tencent Open Platform SDK bundled into the same global APK distributed to EU users with no disclosed Art. 44 transfer mechanism to a PIPL/National-Security-Law jurisdiction, a RECORD_AUDIO permission with no identifiable implementation anywhere in 27 dex files or native libraries, a targetSdkVersion three Android releases out of date, an account-visibility permission set exceeding what OAuth login requires, and a calendar-read plus high-frequency-sensor permission pairing with no confirmed feature behind it.

Across thirteen written notices over ninety-one days, the only non-automated reply this case produced, from appsecurity@booking.com on 27 July, redirected RFI-IRFOS to the company's HackerOne bug-bounty programme instead of engaging with any of the three GDPR questions asked. RFI-IRFOS declined the redirect the same day, in writing, explaining that a coordinated GDPR disclosure with a fixed public-interest embargo is not equivalent to a bug-bounty submission queue. Every other inbound message across the case was either an identical automated acknowledgment from dataprotectionoffice@booking.com or a delivery-failure bounce, legal@booking.com's Google Group bounced on every attempt from 27 June onward, and the Dutch Autoriteit Persoonsgegevens bcc on the original R1 bounced immediately as well. No Data Protection Officer was ever named, and none of RFI-IRFOS's five standing questions, on the RECORD_AUDIO permission's purpose, the WeChat/Tencent transfer mechanism, whether certificate pinning has since been added, whether the lead supervisory authority was notified under Art. 33, or whether a Transfer Impact Assessment covers the Tencent SDK, ever received an answer.

Scope: Static analysis of the publicly downloaded production Booking.com Android APK (v32.7.102), via apktool, smali inspection, string extraction, manifest review, and native library analysis, on an authorized test device, only. No Booking.com account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to appsecurity@booking.com, with legal@booking.com (a Google Group) bouncing on every attempt from 27 June onward and never delivering, dataprotectionoffice@booking.com added from 27 July after being located on Booking.com's own privacy policy page, cc press@booking.com and legal@booking.com, bcc/cc across the sequence to the Austrian Datenschutzbehoerde and CERT.at, and a Dutch Autoriteit Persoonsgegevens bcc on the original R1 that bounced immediately. Across thirteen written notices over ninety-one days, the only non-automated inbound reply, from appsecurity@booking.com on 27 July, redirected RFI-IRFOS to Booking.com's HackerOne bug-bounty programme rather than answering any of the three GDPR questions asked; RFI-IRFOS declined the same day, explaining that a bug-bounty triage queue is not the correct venue for a formal Art. 83 disclosure. No named Art. 37 DPO, no substantive answer to any finding, and no further human reply of any kind was received afterward.

ID	Severity	Title
C1	CRITICAL	Firebase/OAuth API key hardcoded in the production APK
C2	CRITICAL	Zero certificate pinning across all payment and reservation traffic
C3	CRITICAL	WeChat/Tencent SDK (181 classes) in the global APK – EU user data routed to Chinese infrastructure
H1	HIGH	RECORD_AUDIO permission with no identifiable implementation
H2	HIGH	targetSdkVersion 31 (Android 12) in 2026
H3	HIGH	GET_ACCOUNTS, MANAGE_ACCOUNTS, and AUTHENTICATE_ACCOUNTS declared together
H4	HIGH	READ_CALENDAR and HIGH_SAMPLING_RATE_SENSORS – scope beyond booking

Subject & Operator Analysis

Booking.com B.V. is headquartered in Amsterdam, Netherlands, and operates as a subsidiary of Booking Holdings Inc. (NASDAQ: BKNG). The Dutch Autoriteit Persoonsgegevens is named in RFI-IRFOS's correspondence as the lead EU supervisory authority for Booking.com B.V.

Findings

C1: Firebase/OAuth 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

Google API key AIzaSyCecagEEJNckS_25xBvdfmgeieLoGy_E2o and Firebase project booking-oauth (database https://booking-oauth.firebaseio.com) are embedded in the production APK and extractable in under 60 seconds; the project name indicates these credentials power Booking.com's OAuth authentication infrastructure.

No reply of any kind, substantive or otherwise, addressed this finding across thirteen notices.

Impact: OAuth-authentication infrastructure's attack surface cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Rotate the exposed key, confirm Firestore/RTDB security rules are deny-by-default, and enforce App Check for this project.

C2: Zero certificate pinning across all payment and reservation 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

No network_security_config.xml and no OkHttp pin hashes were found anywhere in the binary. Certificate pinning is absent across all API connections, including Braintree (247 classes), PayPal (115 classes), Venmo, and Booking.com's own reservation backend.

Hotel and airport Wi-Fi, an untrusted network by default, is the primary realistic attack surface for a travel application; a machine-in-the-middle position on such a network can intercept or alter payment and reservation traffic. No reply of any kind addressed this finding.

Impact: Payment and reservation traffic is susceptible to interception or manipulation by any attacker positioned on the same untrusted network as the user.

Fix: Implement certificate pinning for all payment-processor and reservation-backend connections.

C3: WeChat/Tencent SDK (181 classes) in the global APK – EU user data routed to Chinese infrastructure

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

com.tencent.mm.opensdk (WeChat Open Platform SDK, 181 smali classes, confirmed WeChat Login/Share/Pay/Mini-Program components) is bundled into the same global APK distributed to all users worldwide, including EU residents, and initializes and performs device fingerprinting against Tencent's servers regardless of whether WeChat is installed.

Tencent is subject to China's National Security Law and PIPL; China has no EU adequacy decision. No Art. 44-49 transfer mechanism, adequacy decision, standard contractual clauses, or transfer impact assessment, is disclosed, and EU users are not informed that device data flows to Tencent. No reply of any kind addressed this finding.

Impact: EU users' device data may be transmitted to a PRC-jurisdiction recipient with no disclosed lawful transfer mechanism.

Fix: Separate the WeChat SDK into a China-market-only build flavor, or disclose Tencent explicitly with a valid Art. 44 transfer mechanism for the global build.

H1: RECORD_AUDIO permission with no identifiable implementation

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

android.permission.RECORD_AUDIO is declared, but full static analysis across 27 dex files and all native libraries found no VOIP SDK, no AudioRecord/MediaRecorder calls, and no voice-search implementation; no disclosed purpose exists in Booking.com's privacy notice.

This is either dead code from a removed feature or a server-activated capability RFI-IRFOS cannot verify externally. No reply of any kind addressed this finding.

Impact: A microphone-access permission is held with no disclosed, verifiable purpose.

Fix: Remove the RECORD_AUDIO permission if the feature it supported was removed, or disclose the feature it activates.

H2: targetSdkVersion 31 (Android 12) in 2026

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

The app targets Android 12, missing three major SDK security releases: Android 13's permission auto-reset and granular media access, Android 14's strict foreground-service types and health-data protections, and Android 15's private space and stricter intent handling. WRITE_EXTERNAL_STORAGE is still declared despite being ineffective on Android 10 and later.

No reply of any kind addressed this finding.

Impact: Users run without three generations of platform-level privacy and security hardening that a current targetSdkVersion would provide by default.

Fix: Raise targetSdkVersion to the current Android release and remove permissions ineffective on modern Android versions.

H3: GET_ACCOUNTS, MANAGE_ACCOUNTS, and AUTHENTICATE_ACCOUNTS declared together

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

These three account-management permissions together grant visibility into every account registered on the device, Gmail addresses, Microsoft accounts, and social logins, beyond what hotel booking or OAuth login requires; this is not disclosed as a processing activity.

No reply of any kind addressed this finding.

Impact: Device-wide account visibility exceeds the stated purpose of authenticating a single Booking.com login.

Fix: Restrict account access to the specific account type used for OAuth login rather than device-wide account visibility.

H4: READ_CALENDAR and HIGH_SAMPLING_RATE_SENSORS – scope beyond booking

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

WRITE_CALENDAR is justified, the app writes bookings to the calendar, but READ_CALENDAR, reading a user's existing appointments, is not, and can reveal employer, medical appointments, relationships, and travel patterns. HIGH_SAMPLING_RATE_SENSORS (above 200Hz) is declared with no confirmed implementation found.

No reply of any kind addressed this finding.

Impact: Calendar-read access and high-frequency sensor access together exceed what a booking application's stated purpose requires and could support behavioral profiling.

Fix: Remove READ_CALENDAR if only calendar-write is used, and remove HIGH_SAMPLING_RATE_SENSORS unless tied to a disclosed, active feature.

One Reply in Ninety-One Days, and It Was a Redirect

The only non-automated reply this case produced in ninety-one days, from appsecurity@booking.com on 27 July, directed RFI-IRFOS to Booking.com's HackerOne bug-bounty programme rather than answering any of the three GDPR questions on the table. RFI-IRFOS declined the same day, explaining in writing that a formal Art. 83 coordinated disclosure with a fixed 90-day public-interest embargo is not the same instrument as a bug-bounty triage submission, and restated the request for a joint DPO and security-leadership review. No further human reply of any kind arrived afterward. Every other inbound message was either an identical automated acknowledgment from dataprotectionoffice@booking.com or a delivery-failure bounce, legal@booking.com's Google Group bounced on every attempt from 27 June onward, and the Dutch Autoriteit Persoonsgegevens bcc on the original R1 bounced immediately.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded OAuth/Firebase key in the production APK
C2	GDPR Art. 32(1)(a)	No certificate pinning across payment and reservation traffic
C3	GDPR Art. 13(1)(e)(f), Art. 44	Undisclosed WeChat/Tencent transfer to a PRC-jurisdiction recipient
H1	GDPR Art. 5(1)(b), Art. 6, Art. 13	Microphone permission with no disclosed purpose
H2	GDPR Art. 25(1)	Outdated targetSdkVersion missing current platform protections
H3	GDPR Art. 5(1)(c), Art. 13	Device-wide account visibility beyond stated purpose
H4	GDPR Art. 5(1)(b)(c), Art. 13	Calendar-read and high-frequency sensor access beyond booking's stated purpose

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to appsecurity@booking.com, 3 CRITICAL + 4 HIGH findings; Dutch AP bcc bounces immediately
2026-06-27	Day-7 follow-up adds legal@booking.com (bounces, Google Group) and press@booking.com in cc, bcc Austrian DSB and CERT.at
2026-07-27	dataprotectionoffice@booking.com added after being located on Booking.com's own privacy policy page; appsecurity@booking.com replies, redirecting to HackerOne; RFI-IRFOS declines the same day
2026-08-31	'Seven Days Since Our Last Message, One Reply in Seventy-Two Days' follow-up
2026-09-12	'Eighty-Four Days, Payment Traffic Still Unpinned' follow-up restates all findings, discloses weekly SHA-256 re-pull of the binary during embargo, confirms 19 September 2026 embargo
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Name an Art. 37 Data Protection Officer and a functional escalation path distinct from the HackerOne bug-bounty programme for formal GDPR disclosures.
- Implement certificate pinning across Braintree, PayPal, Venmo, and the reservation back-end.
- Separate the WeChat/Tencent SDK into a China-market-only build, or disclose it explicitly with a valid Art. 44 transfer mechanism.
- Rotate the exposed Firebase/OAuth key and confirm deny-by-default security rules with App Check enforced.
- Disclose the purpose of the RECORD_AUDIO permission or remove it.

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, 6, 13, 25, 32, 44. REF BOOKING-2026-R1.