FLIGHT SCANNER

COOKIES POLICY

COOKIE CONSENT POLICY

Flight Corner Pty Ltd, trading as Flight Scanner Australia

(IATA No. 02368575, ABN 91 694 615 702) — www.flightscanner.co.za

Policy Version: 1.0 **Effective Date:** 1 August 2026 **Review Cycle:** Every 6 months or upon addition of a new cookie/tracking technology

1. Purpose

This policy sets out how Flight Scanner collects consent for cookies and similar tracking technologies used on **www.flightscanner.co.za** and the technical and legal standard applied across all markets served (Middle East, South Asia, Southeast Asia, Africa, and Australia).

Because Flight Scanner serves customers across multiple jurisdictions, this policy applies the strictest applicable standard (EU GDPR / ePrivacy) globally, rather than maintaining separate region-by-region rules. Meeting the GDPR standard also satisfies the requirements of POPIA (South Africa) and the Australian Privacy Act.

2. Cookie Categories

Category	Purpose	Examples	Consent required?
Essential	Session handling, booking cart, payment security, fraud prevention	Session ID, CSRF token, Stripe fraud signals	**No — always active**
Functional	Remembers language, currency, search preferences	Locale cookie, currency cookie	**Yes — opt-in**
Analytics	Understand site usage and improve performance	Google Analytics, Hotjar	**Yes — opt-in**
Marketing	Ad targeting, retargeting, conversion tracking	Meta Pixel, Google Ads tag	**Yes — opt-in**
Payment / BNPL partners	Enable checkout with third-party payment and BNPL providers	Stripe, WeChat Pay, Tabby, Tamara, Splitit, Atome	**No — essential to checkout function selected by user**

3. Banner Behaviour

3.1 Display format

- Non-blocking bar (does not cover the search box or booking flow)

- Three clear options: Accept All / Reject Non-Essential / Customise
- Link through to the full Cookie Policy page for category-level detail

3.2 When the banner shows

The banner is NOT shown on every visit. It only appears when:

- The visitor has no stored consent record (first-time visitor, or cookies cleared)
- The stored consent has expired (see 3.3)
- The `policy_version` has changed because a new tracker or supplier was added

3.3 Consent expiry

Stored consent is valid for 6 months from the date it was given. This is a deliberately conservative window (GDPR guidance allows up to 12 months) chosen because Flight Scanner is actively adding new suppliers and payment integrations, and shorter expiry reduces the risk of stale consent being relied upon.

4. Technical Implementation

Consent is stored as a first-party, signed cookie (not only local Storage, so it can also be read server-side) with the following structure:

```
{ "consent": true, "categories": ["functional","analytics"], "timestamp":
"2026-08-01T00:00:00Z", "policy_version": "1.0" }
```

On every page load, the site checks this record before initialising any non-essential script. Analytics, marketing, and third-party embed scripts are gated behind the consent check and only fire once the relevant category has been accepted. See the accompanying code files (`consent.ts` and `Cookie Banner.tsx`) for the reference implementation for the Next.js stack.

5. Re-Consent Triggers

The banner is automatically re-shown, and previously granted consent is disregarded, when any of the following occur:

- 6 months have elapsed since consent was given
- A new cookie category or third-party tracker is added (e.g. a new BNPL provider's pixel, a new analytics tool) — triggered by incrementing `policy_version`
- The visitor clears cookies or uses a new device/browser

6. Governance

- Review this policy every 6 months, or immediately when a new supplier/integration is added to the site
- Maintain a version log recording what changed and when, for KYC and audit purposes