CookieJar

The Cookie Compliance Audit Checklist

A 32-point self-audit covering GDPR, CCPA, LGPD and 40+ regimes. Use this checklist before your next compliance review or DPA inquiry.

1. Cookie discovery & inventory

- ■ Run a full-site cookie scan covering all subdomains and authenticated areas
- ■ Categorize every cookie (strictly necessary, functional, analytics, advertising)
- ■ Document cookie purpose, vendor, retention period, and data-sharing destination
- ■ Identify cookies set by third-party scripts (chat widgets, analytics, embeds)
- ■ Schedule recurring scans (weekly recommended) to detect new trackers

2. Banner & UX

- ■ Show banner before any non-essential cookie or tracker fires
- ■ Provide equally prominent 'Accept' and 'Reject' buttons (GDPR)
- ■ Offer granular per-category opt-in/opt-out controls
- ■ Make 'Withdraw consent' as easy as giving consent
- ■ Avoid pre-ticked checkboxes for non-essential categories
- ■ Localize banner copy by visitor region and language

3. Consent records

- ■ Store proof of consent (timestamp, banner version, choice) for every visitor
- ■ Retain records for at least 24 months (GDPR best practice)
- ■ Make consent records exportable for regulators on demand
- ■ Log consent withdrawals with the same detail as opt-ins

4. Multi-regime coverage

- ■ GDPR / ePrivacy: opt-in required before non-essential cookies
- ■ CCPA / CPRA: 'Do Not Sell or Share My Personal Information' link visible
- ■ LGPD (Brazil): legal basis recorded for each processing activity
- ■ PIPEDA (Canada): meaningful consent with plain-language explanation
- ■ POPIA (South Africa): data subject rights surfaced in policy
- ■ Detect visitor region server-side and apply the correct legal basis

5. Cookie policy & transparency

- ■ Publish a cookie policy that auto-updates from your latest scan
- ■ Link the policy from the banner and the site footer
- ■ Disclose all third-party recipients of cookie data
- ■ List retention period and legal basis per category

6. Vendor & tag management

- ■ Block third-party tags until consent is recorded (server-side preferred)
- ■ Integrate consent state with Google Consent Mode v2
- ■ Audit your tag manager containers for unconsented fires
- ■ Maintain a Data Processing Agreement (DPA) with each vendor

7. Reporting & audit readiness

- ■ Be able to produce a DPA-ready compliance report in under 1 hour
- ■ Track accept-rate by region, banner version, and traffic source
- ■ Export CSV/PDF reports without per-export fees or row caps
- ■ Maintain an immutable change log of banner and policy edits

Score yourself

28–32 checked: Audit-ready. 20–27: Address gaps within 30 days. Under 20: High regulatory risk — prioritize remediation now.