

PRIVACY COMPLIANCE

Consent Management Vendor Selection Checklist

Score 6 CMPs across 42 criteria and pick the right one in
an afternoon — not three weeks of demos

✓ Print-optimized ✓ Expert-curated ✓ Actionable tips

Consent Management Vendor Selection Checklist

Score 6 CMPs across 42 criteria and pick the right one in an afternoon — not three weeks of demos

Consent Management Vendor Selection Checklist

Score 6 CMPs across 42 criteria and pick the right one in an afternoon — not three weeks of demos

Choosing a Consent Management Platform (CMP) is a 1-3 year commitment that touches legal, engineering, and marketing. Pick wrong and you inherit slow banners, broken Consent Mode, surprise per-domain pricing, and a migration project later. This checklist gives you a weighted scorecard, the exact questions to ask on every demo, and the red flags that disqualify a vendor on the spot.

Time to complete: ~3 hours including two trials. Reviewers needed: one engineer, one person who owns legal/privacy.

How to Use This Checklist

1. **Shortlist 3-6 vendors.** Common ones: GetCookies, Cookiebot, OneTrust, iubenda, CookieYes, Termly, Osano, Usercentrics, Klaro (open-source).
2. **Score each criterion 0-3** using the rubric below. Multiply by the section weight.
3. **Disqualify on any red flag** before you bother scoring — those are deal-breakers, not trade-offs.
4. **Trial the top 2** on a real page for 48 hours before signing anything.

Scoring Rubric

Score	Meaning
0	Not offered, or broken in trial
1	Present but weak / heavy manual work
2	Solid, meets the requirement
3	Best-in-class, exceeds the requirement

A vendor needs an average of **≥2.0 overall** AND **zero red flags** to be a safe choice.

Hard Red Flags (Disqualify Immediately)

- ☐ Banner cannot show a **"Reject All"** button with equal prominence to "Accept All" (illegal in the EU; CNIL, Garante, and the EDPB all require it)
- ☐ Non-essential cookies/tags **fire before consent** in your trial (open DevTools → Application → Cookies in incognito)

- ☐ No **Google Consent Mode v2** support (required since March 2024 for Google Ads/Analytics in the EEA)
 - ☐ No exportable, timestamped **consent proof** (you can't defend an audit without it)
 - ☐ Pricing is **per-domain with no warning** and you run multiple domains/subdomains
 - ☐ Banner adds **>50ms to LCP** or injects render-blocking JS (test in Lighthouse / WebPageTest)
 - ☐ No **Data Processing Agreement (DPA)** available, or the vendor stores consent logs outside your required region
-

Section 1 — Cookie & Tag Discovery (Weight: 25%)

- ☐ **1.1** Automatic recurring cookie scanner (not a one-time scan) — *ask the cadence: weekly is the floor*
- ☐ **1.2** Detects cookies set by third-party tags and iframes, not just first-party
- ☐ **1.3** Auto-categorizes into Necessary / Functional / Analytics / Marketing with editable mapping
- ☐ **1.4** Flags **new/unknown cookies** since the last scan and alerts you
- ☐ **1.5** Maintains a maintainable cookie register you can export to CSV

Demo question: "Run a live scan of my staging site right now — show me the new-cookie diff from the last scan."

Section 2 — Banner & Consent UX (Weight: 20%)

- ☐ **2.1** Equal-weight Accept All / Reject All buttons (same size, color, position)
- ☐ **2.2** Granular per-category toggles in a preferences modal
- ☐ **2.3** No pre-ticked boxes; consent defaults to off for non-essential
- ☐ **2.4** Persistent "Manage cookies" link for re-consent (footer or floating button)
- ☐ **2.5** Full visual customization (CSS / theme) without paying for "custom branding" tier
- ☐ **2.6** WCAG 2.1 AA: keyboard-navigable, screen-reader labels, visible focus states

Demo question: "Show me the default banner with no styling. Is Reject All already equal to Accept All out of the box?"

Section 3 — Technical Integration (Weight: 20%)

- ☐ **3.1** Google Consent Mode v2 (basic + advanced) with documented setup
- ☐ **3.2** Google Tag Manager consent integration / native template
- ☐ **3.3** IAB TCF 2.2 support (only required if you serve programmatic ads)
- ☐ **3.4** Server-side / API consent retrieval for SSR frameworks (Next.js, Nuxt, Remix)
- ☐ **3.5** Blocks tags **by default** until consent (not "best-effort" client-side)
- ☐ **3.6** Async / non-render-blocking script; banner paints in <1s
- ☐ **3.7** Real SDK/snippet docs for your stack (React, Vue, WordPress, Shopify, etc.)

Demo question: "Paste me the exact GTM + Consent Mode v2 setup doc. How many steps to block GA4 before consent?"

Section 4 — Compliance Coverage (Weight: 15%)

- ☐ **4.1** Geo-targeting: GDPR for EEA/UK, opt-out model for US states, configurable per region

- ☐ **4.2** US state laws: CCPA/CPRA "Do Not Sell or Share" + Global Privacy Control (GPC) signal honored
- ☐ **4.3** Multi-language banners that match site locale automatically
- ☐ **4.4** Re-consent prompts when your policy or vendor list changes
- ☐ **4.5** Auto-generated, always-current cookie policy / disclosure table

Demo question: "Show me the same site rendering an EU banner and a California opt-out banner based on visitor region."

Section 5 — Records, Audit & Reporting (Weight: 10%)

- ☐ **5.1** Timestamped consent logs with version of the policy consented to
- ☐ **5.2** Exportable consent records (CSV/API) for audits and DSAR responses
- ☐ **5.3** Consent analytics: accept rate, reject rate, by region/page
- ☐ **5.4** Tamper-evident or immutable log storage

Demo question: "Export 10 consent records right now and show me the fields. Can a regulator verify these?"

Section 6 — Commercial & Support (Weight: 10%)

- ☐ **6.1** Pricing scales by **pageviews/sessions**, not per-domain, and you've modeled your real volume
- ☐ **6.2** No surprise overage fees; the published tier covers your traffic
- ☐ **6.3** Signed DPA + clear data residency (EU storage if you need it)
- ☐ **6.4** Documented SLA and support channel that fits your team (email/Slack/priority)
- ☐ **6.5** Migration path documented (you'll thank yourself later)

Demo question: "At [my monthly pageviews] across [N] domains, what's my exact yearly price including overages?"

Scorecard

Fill one row per vendor. **Weighted score = Σ (section average $\times$ weight).**

Vendor	Discovery (25%)	Banner UX (20%)	Integration (20%)	Compliance (15%)	Records (10%)	Commercial (10%)	Red flags?	Weighted total
--------	--------------------	-----------------------	----------------------	---------------------	------------------	---------------------	---------------	-------------------

Decision rule: Eliminate anything with a red flag. Among the rest, the highest weighted total wins. If two are within 0.2, the one with the faster banner and cheaper real-volume price wins.

The 48-Hour Trial Test (do this before signing)

1. Install the banner on **one real page** (staging is fine).
2. Open incognito + DevTools → Application → Cookies. **Before clicking anything**, confirm only essential cookies exist.
3. Run **Lighthouse**. Note the LCP/TBT impact of the banner script.

4. Click **Reject All** → refresh → confirm non-essential cookies are gone and the choice is remembered.
5. Switch your IP/region (VPN) → confirm the banner adapts (EU vs US behavior).
6. **Export consent records** and check they're audit-ready.

Any vendor that fails steps 2, 4, or 6 is out — those are the exact things regulators check.

Why teams pick GetCookies

GetCookies was built to pass every item on this checklist out of the box:

- **Recurring automatic scanner** with new-cookie alerts and auto-categorization
- **Equal-weight Reject All** by default — compliant on install, no config required
- **Google Consent Mode v2 + GTM** native, set up in minutes
- **Geo-targeting** for GDPR, UK GDPR, and US state opt-out (GPC honored)
- **Audit-ready, exportable consent logs** with policy versioning
- **Pageview-based pricing**, no per-domain surprises

Scan your site free → getcookies.co

This checklist is for informational purposes and does not constitute legal advice. Have your legal/privacy owner sign off before launch.