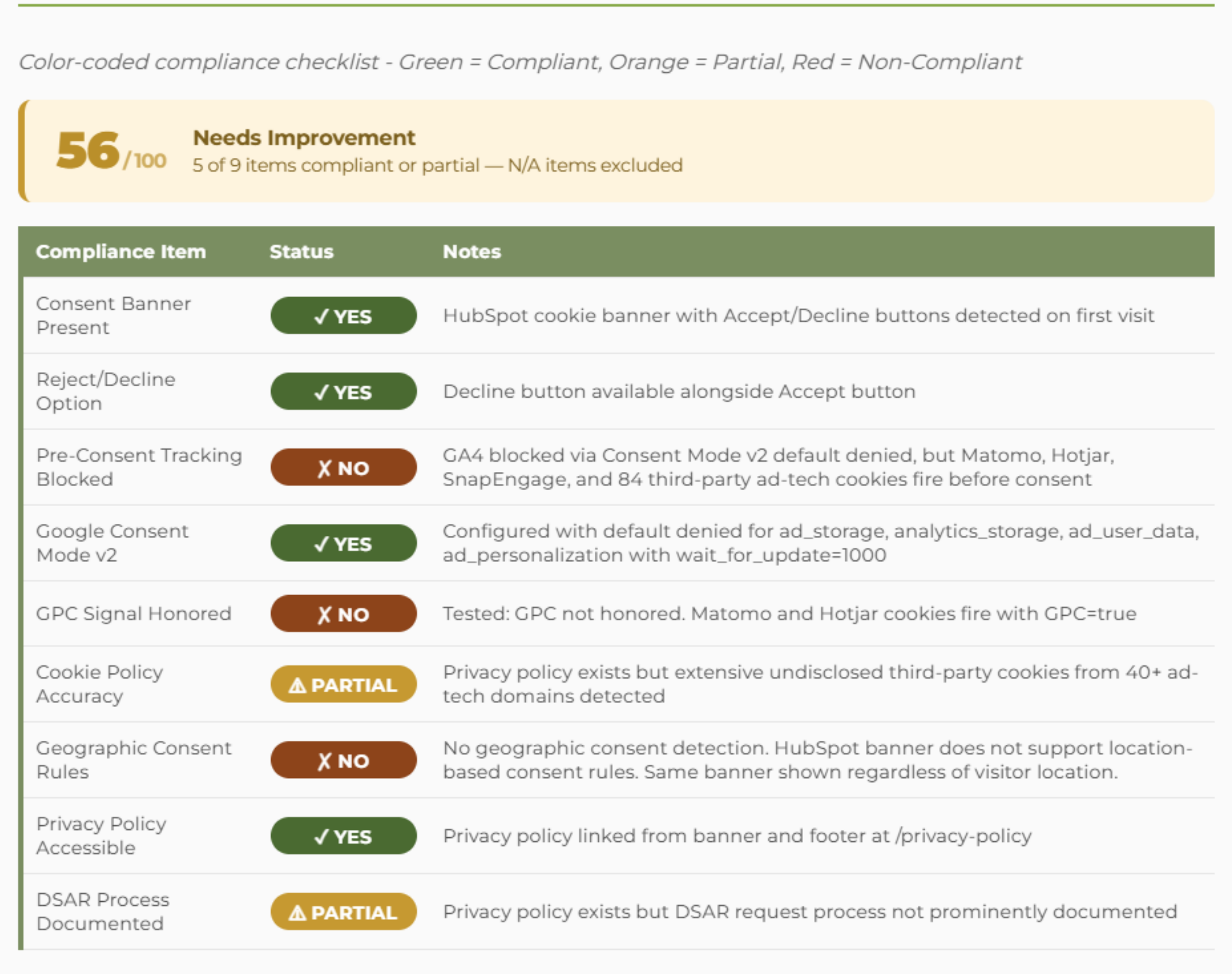
# Your Data Privacy Risk Score & Action Plan

| PREPARED FOR: | [Company Name] |
|---|---|
| Website Domain: | [Your Domain] |

## Compliance Status Summary

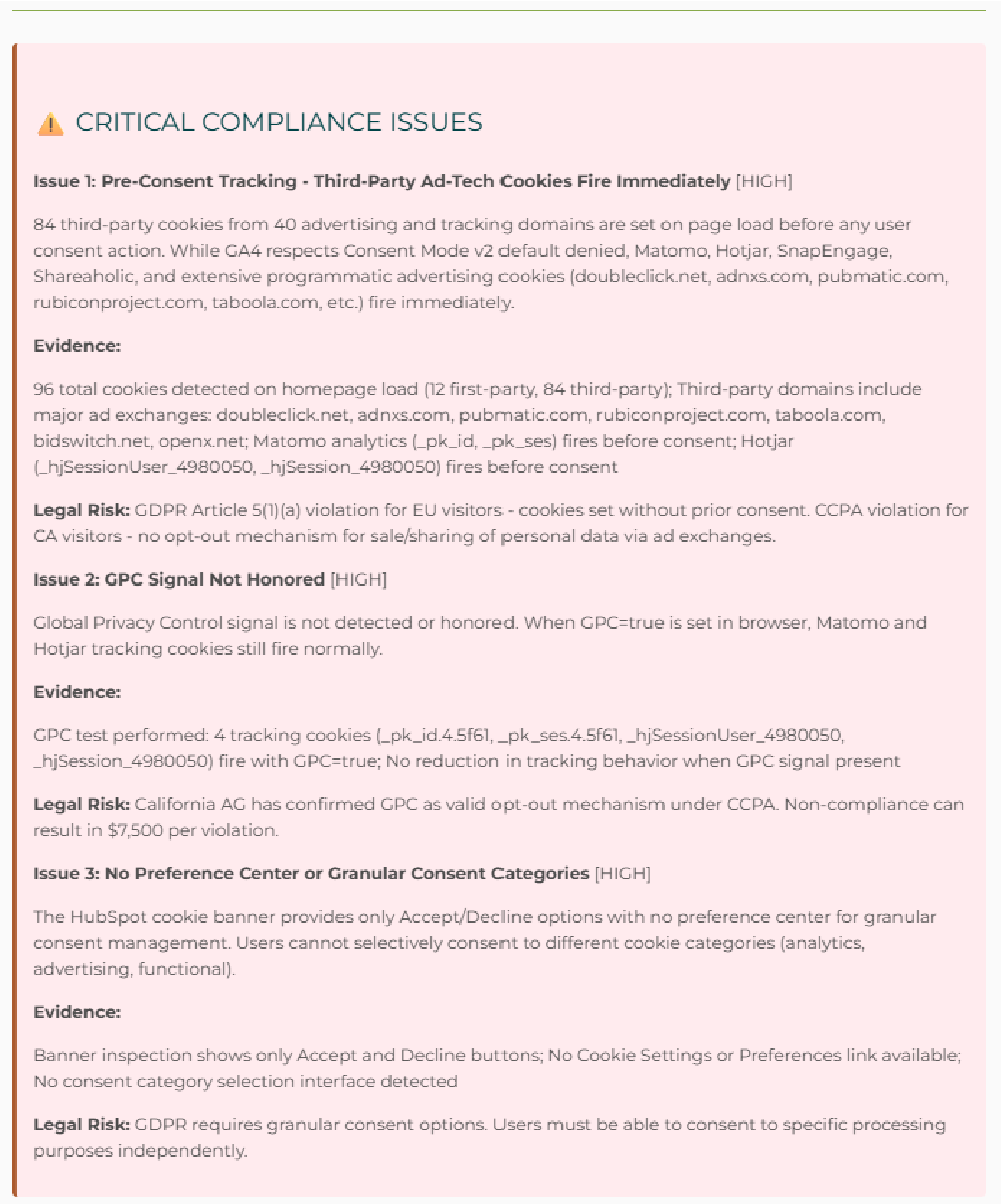


*Color-coded compliance checklist - Green = Compliant, Orange = Partial, Red = Non-Compliant*

**56**/100 **Needs Improvement**
5 of 9 items compliant or partial — N/A items excluded

| Compliance Item | Status | Notes |
|---|---|---|
| Consent Banner Present | ✓ YES | HubSpot cookie banner with Accept/Decline buttons detected on first visit |
| Reject/Decline Option | ✓ YES | Decline button available alongside Accept button |
| Pre-Consent Tracking Blocked | ✗ NO | GA4 blocked via Consent Mode v2 default denied, but Matomo, Hotjar, SnapEngage, and 84 third-party ad-tech cookies fire before consent |
| Google Consent Mode v2 | ✓ YES | Configured with default denied for ad_storage, analytics_storage, ad_user_data, ad_personalization with wait_for_update=1000 |
| GPC Signal Honored | ✗ NO | Tested: GPC not honored. Matomo and Hotjar cookies fire with GPC=true |
| Cookie Policy Accuracy | ⚠ PARTIAL | Privacy policy exists but extensive undisclosed third-party cookies from 40+ ad-tech domains detected |
| Geographic Consent Rules | ✗ NO | No geographic consent detection. HubSpot banner does not support location-based consent rules. Same banner shown regardless of visitor location. |
| Privacy Policy Accessible | ✓ YES | Privacy policy linked from banner and footer at /privacy-policy |
| DSAR Process Documented | ⚠ PARTIAL | Privacy policy exists but DSAR request process not prominently documented |

# Critical Compliance Issues Detected



## ⚠ CRITICAL COMPLIANCE ISSUES

**Issue 1: Pre-Consent Tracking - Third-Party Ad-Tech Cookies Fire Immediately** [HIGH]

84 third-party cookies from 40 advertising and tracking domains are set on page load before any user consent action. While GA4 respects Consent Mode v2 default denied, Matomo, Hotjar, SnapEngage, Shareaholic, and extensive programmatic advertising cookies (doubleclick.net, adnxs.com, pubmatic.com, rubiconproject.com, taboola.com, etc.) fire immediately.

**Evidence:**

96 total cookies detected on homepage load (12 first-party, 84 third-party); Third-party domains include major ad exchanges: doubleclick.net, adnxs.com, pubmatic.com, rubiconproject.com, taboola.com, bidswitch.net, openx.net; Matomo analytics (_pk_id, _pk_ses) fires before consent; Hotjar (_hjSessionUser_4980050, _hjSession_4980050) fires before consent

**Legal Risk:** GDPR Article 5(1)(a) violation for EU visitors - cookies set without prior consent. CCPA violation for CA visitors - no opt-out mechanism for sale/sharing of personal data via ad exchanges.

**Issue 2: GPC Signal Not Honored** [HIGH]

Global Privacy Control signal is not detected or honored. When GPC=true is set in browser, Matomo and Hotjar tracking cookies still fire normally.

**Evidence:**

GPC test performed: 4 tracking cookies (_pk_id.4.5f61, _pk_ses.4.5f61, _hjSessionUser_4980050, _hjSession_4980050) fire with GPC=true; No reduction in tracking behavior when GPC signal present

**Legal Risk:** California AG has confirmed GPC as valid opt-out mechanism under CCPA. Non-compliance can result in $7,500 per violation.

**Issue 3: No Preference Center or Granular Consent Categories** [HIGH]

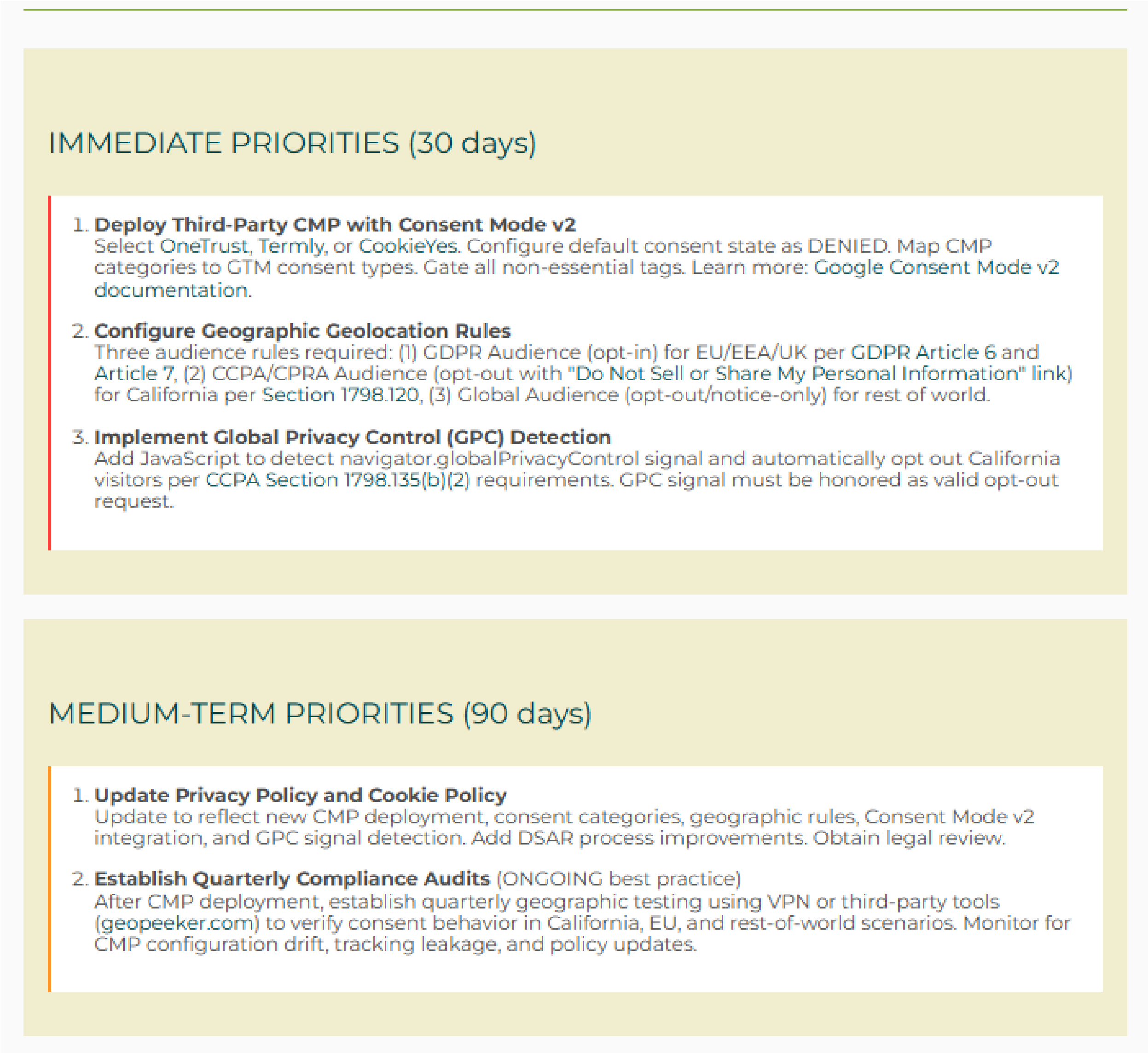
The HubSpot cookie banner provides only Accept/Decline options with no preference center for granular consent management. Users cannot selectively consent to different cookie categories (analytics, advertising, functional).

**Evidence:**

Banner inspection shows only Accept and Decline buttons; No Cookie Settings or Preferences link available; No consent category selection interface detected

**Legal Risk:** GDPR requires granular consent options. Users must be able to consent to specific processing purposes independently.

# Recommendations



## IMMEDIATE PRIORITIES (30 days)

1. **Deploy Third-Party CMP with Consent Mode v2**
   Select OneTrust, Termly, or CookieYes. Configure default consent state as DENIED. Map CMP categories to GTM consent types. Gate all non-essential tags. Learn more: Google Consent Mode v2 documentation.
2. **Configure Geographic Geolocation Rules**
   Three audience rules required: (1) GDPR Audience (opt-in) for EU/EEA/UK per GDPR Article 6 and Article 7, (2) CCPA/CPRA Audience (opt-out with "Do Not Sell or Share My Personal Information" link) for California per Section 1798.120, (3) Global Audience (opt-out/notice-only) for rest of world.
3. **Implement Global Privacy Control (GPC) Detection**
   Add JavaScript to detect navigator.globalPrivacyControl signal and automatically opt out California visitors per CCPA Section 1798.135(b)(2) requirements. GPC signal must be honored as valid opt-out request.

## MEDIUM-TERM PRIORITIES (90 days)

1. **Update Privacy Policy and Cookie Policy**
   Update to reflect new CMP deployment, consent categories, geographic rules, Consent Mode v2 integration, and GPC signal detection. Add DSAR process improvements. Obtain legal review.
2. **Establish Quarterly Compliance Audits** (ONGOING best practice)
   After CMP deployment, establish quarterly geographic testing using VPN or third-party tools (geopeeker.com) to verify consent behavior in California, EU, and rest-of-world scenarios. Monitor for CMP configuration drift, tracking leakage, and policy updates.