OPERATIONAL STANDARD

Privacy Policy & CCPA/CPRA Standard

BRSG Compliance Standard · v1.0 · effective 2026-06-25 · standards.billricestrategy.com

Privacy Policy & CCPA/CPRA Standard

Owner: Bill Rice (BRC LLC d/b/a Bill Rice Strategy Group) **Version:** v1.0 — 2026-06-25 **Scope:** Every BRSG-owned property that collects personal information from visitors — through newsletter signups, gated downloads, lead-capture forms, contact forms, or analytics. Defines the baseline privacy policy every such property must publish, and the CCPA/CPRA elements it must contain. **Status:** Deployable. This standard exists to close the gap identified in the 2026-06-25 owned-property compliance audit, where the majority of live properties collected personal information with no working privacy policy.

1. Why this standard exists

Most BRSG content properties run on the same stack and follow the same playbook: publish useful financial content, capture email through a newsletter or a gated lead magnet, and in some cases route a consumer to a lender or provider. Every one of those flows collects personal information. Under California's Consumer Privacy Act as amended by the CPRA, a business that collects California residents' personal information must publish a privacy policy describing what it collects, how it uses and shares it, and the rights consumers have — and must offer a mechanism to opt out of the "sale" or "sharing" of that information. Analogous laws now exist in numerous other states, and the federal CAN-SPAM Act governs the newsletter relationship.

A property that collects email or form data with no posted privacy policy is exposed regardless of how scrupulously it actually handles data. This standard sets the floor: what every data-collecting BRSG property must publish, and what that policy must say.

2. When a privacy policy is required

A privacy policy is **required** on any BRSG property that does any of the following:

- Collects email addresses (newsletter, gated content, contact form).
- Operates any lead-capture or intake form.
- Routes or transfers consumer data to a third party (e.g., a lender finder).
- Runs analytics or advertising tags that collect identifiers (e.g., Google Analytics, GTM, pixels).

In practice this means **every live BRSG property that is not a pure static brochure** needs one. When in doubt, publish one.

3. Required elements

Every BRSG privacy policy must contain, at minimum:

1. **Categories of personal information collected.** Plainly stated — e.g., identifiers (name, email, IP address), internet activity (pages viewed, referral source, device/browser), and any data entered into forms. Map to the CCPA statutory categories where practical.
2. **Sources of the information.** Directly from the visitor (forms) and automatically (analytics, server logs).
3. **Purposes of use.** Why each category is collected (deliver the newsletter, respond to inquiries, measure traffic, connect a consumer with a provider).
4. **Categories of third parties.** Who the data is shared with, by category — service providers/processors (hosting, analytics, email delivery, CMS) and, where applicable, the providers a lead is routed to. Name the key processors.
5. **Sale / sharing disclosure + opt-out.** A clear statement of whether the property sells or "shares" (for cross-context behavioral advertising) personal information. If it does **not**, say so explicitly — and note that the no-share statement covers analytics/advertising tags, because those can constitute "sharing" under CPRA even with no money changing hands. If it **does** (e.g., a lender-routing flow that transfers data for value), provide a working **"Do Not Sell or Share My Personal Information"** link or mechanism.

6. **Consumer rights (CCPA/CPRA).** A California-specific section enumerating the rights to know/access, delete, correct, opt out of sale/sharing, limit use of sensitive information, and non-discrimination for exercising rights — and how to exercise them.
7. **Contact method.** An email address (and, preferably, a physical mailing address) for privacy requests.
8. **Data retention.** How long categories of data are kept, or the criteria used to determine it.
9. **Children.** A statement that the property does not knowingly collect information from children under 13 (COPPA) / 16 (CPRA sensitive threshold).
10. **Effective date and changes.** The policy's effective/last-updated date and how updates are communicated.

4. Notice at collection

CPRA requires notice **at or before** the point of collection. On any page with a lead-capture or intake form, place a short notice directly at the form — beneath or beside the submit button — stating what is collected and why, with a link to the full privacy policy. A footer link alone does not satisfy notice-at-collection for an active form.

5. Deployment

1. **Publish the policy** at a stable path (`/privacy` is the canonical slug for the BRSG fleet — avoid publishing at `/privacy-policy` if footer links point to `/privacy`, and vice versa; the link and the page must match).
2. **Link it site-wide** in the footer of every page.
3. **Add notice-at-collection** beneath every active form (§ 4).
4. **Templated rollout.** Because the BRSG content hubs share a Next.js + Sanity stack, deploy a single privacy-policy page component and footer-link component across the fleet rather than authoring each site by hand. This is the efficient path to closing the gap fleet-wide.
5. **Verify after deploy.** Confirm the published path returns 200, the footer link resolves to it (no 404), and the notice-at-collection renders beneath each form.

6. Maintenance

- Review each property's privacy policy at least annually and whenever a new data flow is added (new form field, new analytics/advertising tag, new third-party routing).
- Adding a **phone field** to any form triggers the TCPA/Lead Consent Standard in addition to this one.
- Adding a **lead-routing or data-transfer flow** that moves consumer data to a third party for value requires re-checking the sale/share disclosure and the Do-Not-Sell/Share mechanism.

7. Legal basis

- **California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq., as amended by the CPRA.** The controlling framework for the required elements above, the notice-at-collection obligation, and the sale/sharing opt-out.
- **Other state privacy laws.** A growing set of states (e.g., Virginia, Colorado, Connecticut, and others) impose comparable notice and rights obligations; a CCPA/CPRA-grade policy substantially covers them.
- **CAN-SPAM Act, 15 U.S.C. § 7701 et seq.** Governs the commercial-email relationship created by newsletter signups (accurate headers, working unsubscribe, postal address).
- **COPPA, 15 U.S.C. § 6501 et seq.** Underlies the children's-data statement.

Version History

VERSION	DATE	CHANGE
v1.0	2026-06-25	Initial standard. Defines required privacy-policy elements, notice-at-collection, and fleet deployment. Issued to close the privacy gap found in the 2026-06-25 owned-property audit.

When this standard is cited in a contract or counsel memo, cite it **by version** (e.g., "Privacy Policy & CCPA/CPRA Standard v1.0"). The version and date in the header above are

authoritative.