

# Website Risk Snapshot

Point-in-time observable signal assessment

Risk level: Medium

Website	example.com
Timestamp (UTC)	2026-02-12T22:47:27.318Z
Report ID	8878a4974ba7
Integrity hash	c7eb98c339a3aa9785668b1735f...

Observable signals only. Not legal advice. Not certification. Applies only at the recorded timestamp.

WebsiteRiskCheck.com • Report ID: 8878a4974ba7 • Timestamp (UTC): 2026-02-12T22:47:27.318Z

Verify: /verify/c7eb98c339a3aa9785668b1735f5d685da13c22caabbfe470679e2452ef8db8c

# Executive summary

## Risk level: Medium

This snapshot shows some risk-relevant signals and/or missing indicators that are commonly expected on customer-facing websites. It does not prove non-compliance, but it suggests potential gaps worth reviewing.

## Risk register

A structured view of key detectable risks based on scope-locked signals. Probability/impact are indicative only and not legal conclusions.

Risk Category	Risk Description	Probability	Impact
Coverage	Public pages were retrieved for analysis using a scope-locked approach (homepage + standard policy/contact paths).	Rare (1)	Minor (2)
Compliance	One or more standard policy pages were not detected on common public paths (privacy/terms/cookie policy).	Likely (4)	Major (4)
Trust	Contact/business identity signals were not detected on the scanned surface, which can reduce trust and conversion.	Possible (3)	Minor (2)

Note: Scores reflect probability×impact for the register entries above and are independent of the overall risk score.

## Key findings (detectable signals)

- HTTPS: Detected
- Fetch: Successful
- Privacy policy: Not detected
- Terms: Not detected
- Cookie policy: Not detected
- Consent banner indicator: Not detected (heuristic)
- Tracking scripts: None detected
- Cookie vendor signals: None detected
- Forms detected: 0
- Potential personal-data field signals: 0 (heuristic)
- Images missing alt text: 0 of 0
- Contact/identity signals: Not detected

## Notable observations

- Privacy policy was not detected on common public paths.
- Terms were not detected on common public paths.
- Cookie policy was not detected on common public paths.
- No common tracking scripts or cookie vendor signals were detected.
- Contact/business identity signals were not detected on the scanned surface.

WebsiteRiskCheck.com • Report ID: 8878a4974ba7 • Timestamp (UTC): 2026-02-12T22:47:27.318Z

Verify: /verify/c7eb98c339a3aa9785668b1735f5d685da13c22caabbfe470679e2452ef8db8c

# Findings by category

## Connection

- HTTPS: Detected

HTTPS reduces interception risk and is commonly expected for customer-facing websites.

---

## Policies (public-path detection)

- Privacy policy present: Not detected
- Terms present: Not detected
- Cookie policy present: Not detected

Policy presence is detected using a scope-locked approach (homepage links and standard public policy paths). Absence of detection is not proof of absence.

---

## Cookies & tracking (HTML detection)

- Tracking scripts: None detected
- Cookie vendor signals: None detected

Detections are based on observable HTML/script references. If trackers load dynamically, they may not be detected.

---

## Consent indicators (heuristic)

- Cookie/consent banner indicator: Not detected

This is a heuristic signal based on text and DOM patterns and/or the presence of consent vendors. It is not a guarantee.

---

## Forms & data capture (heuristic)

- Forms detected: 0
- Potential personal-data field signals: 0

The personal-data signal is a heuristic count based on common field names (e.g., email, phone, name). It is not a legal classification.

---

## Accessibility signals (heuristic)

- Images missing alt text: 0 of 0
- No accessibility notes recorded by this scan.

Accessibility checks are lightweight and indicative only. A full accessibility review typically requires page coverage and manual testing.

---

## Contact & identity signals

- Contact/business identity signals: Not detected

Detected using simple patterns (email/phone/contact link) on the scanned surface only.

---

WebsiteRiskCheck.com • Report ID: 8878a4974ba7 • Timestamp (UTC): 2026-02-12T22:47:27.318Z

Verify: /verify/c7eb98c339a3aa9785668b1735f5d685da13c22caabbfe470679e2452ef8db8c

## Common next steps (non-prescriptive)

The items below are commonly reviewed when these signals appear. They are provided for general orientation only and are not legal advice.

- Ensure privacy and terms pages are public and linked from the site footer and/or homepage.
- If third-party tracking or cookies are used, review whether consent mechanisms are appropriate for your target regions and audiences.
- Review forms for minimum necessary fields and confirm where submissions are stored and who can access them.
- Add alt text to meaningful images on key pages where missing.
- Ensure visitors can easily find contact or business identity information.
- Re-run a snapshot after major changes (redesign, marketing tag updates, new forms, new third-party embeds).

WebsiteRiskCheck.com • Report ID: 8878a4974ba7 • Timestamp (UTC): 2026-02-12T22:47:27.318Z

Verify: /verify/c7eb98c339a3aa9785668b1735f5d685da13c22caabbfe470679e2452ef8db8c

# Methodology & limitations

## Methodology (this scan)

- Fetches public HTML from the homepage and standard public policy/contact paths (scope-locked).
- Detects common tracking scripts by known patterns in HTML.
- Detects common consent vendors by known patterns in HTML.
- Detects policy presence via homepage links and standard paths (scope-locked).
- Detects banner indicators via DOM/text heuristics (heuristic).
- Detects forms and likely personal-data field signals via field-name heuristics.
- Runs lightweight accessibility checks (e.g., <html lang>, H1 presence, alt text counts).

## Scope and exclusions

- No full-site crawling.
- Public, unauthenticated HTML only (no logins).
- No JavaScript execution or behavioural simulation (no clicking banners, no region toggles).
- No legal judgement, certification, or guarantee of compliance.
- No monitoring over time; this is a single timestamped snapshot.

## Limitations (important)

- Results apply only at the recorded timestamp; websites can change without notice.
- Dynamically loaded or interaction-gated content may not be detected.
- Heuristic signals may produce false positives/negatives depending on implementation.
- Absence of detection is not proof of absence.

WebsiteRiskCheck.com • Report ID: 8878a4974ba7 • Timestamp (UTC): 2026-02-12T22:47:27.318Z

Verify: /verify/c7eb98c339a3aa9785668b1735f5d685da13c22caabbfe470679e2452ef8db8c

# Report verification

This report can be independently verified using its cryptographic fingerprint. The integrity hash is derived from objective fields only, allowing verification that the recorded facts have not been altered.

## Integrity hash (SHA-256)

c7eb98c339a3aa9785668b1735f5d685da13c22caabbfe470679e2452ef8db8c

## Verify this report

</verify/c7eb98c339a3aa9785668b1735f5d685da13c22caabbfe470679e2452ef8db8c>

## What the integrity hash covers

- Target URL/hostname, scan ID, scan timestamp
- Scope-locked coverage notes
- HTTPS signal
- Policy presence signals (privacy/terms/cookie policy)
- Consent indicator signal (cookie banner heuristic)
- Tracking scripts and cookie vendor detections
- Forms detected and personal-data field signals (heuristic counts)
- Accessibility signals (alt text counts, notes)
- Contact/identity signal presence
- Per-page coverage (checked/failed paths where available)



WebsiteRiskCheck.com • Report ID: 8878a4974ba7 • Timestamp (UTC): 2026-02-12T22:47:27.318Z

Verify: /verify/c7eb98c339a3aa9785668b1735f5d685da13c22caabbfe470679e2452ef8db8c