**WebsiteRiskCheck.com**

Immutable point-in-time website snapshot (observable signals)

# Website Risk Snapshot

Sealed PDF deliverable with public verification

**Risk level: Medium**

| | |
|---|---|
| **Website** | example-retail-site.com |
| **Timestamp (UTC)** | 2026-02-10T14:32:00.000Z |
| **Report ID** | SAMPLE-001 |
| **Integrity hash** | b50d49f57a066f6cc6274c743a89… |

Informational snapshot only — not legal advice, certification, or monitoring. Applies only at the recorded timestamp.

# Executive summary

Client-ready snapshot of observable website signals at a fixed timestamp.

**Risk level: Medium**

| | |
|---|---|
| Report ID<br>**SAMPLE-001** | Timestamp (UTC)<br>**2026-02-10T14:32:00.000Z** |
| Coverage<br>**6 page(s) checked**<br>Scope-locked (public paths) | Verification fingerprint<br>**b50d49f57a…988eeb5319**<br>Public integrity check |

Some risk-relevant signals and/or missing public indicators were detected on the scanned surface. This does not prove non-compliance, but it suggests potential gaps worth reviewing.

### Notable observations

- Cookie policy was not detected on common public paths.
- Tracking/cookie vendor signals were detected.
- Forms were detected with potential personal-data field signals (heuristic).
- Some images appear to be missing alt text (7 of 24).

### Key findings (detectable signals)

- HTTPS: Detected
- Privacy policy: Detected
- Terms: Detected
- Cookie policy: Not detected
- Consent banner indicator: Detected (heuristic)
- Tracking scripts: Detected (Google Analytics, Meta Pixel)
- Cookie vendor signals: Detected (OneTrust)
- Forms detected: 3

- Potential personal-data field signals: 2 (heuristic)
- Images missing alt text: 7 of 24
- Contact/identity signals: Detected

# Risk register

Indicative probability×impact scoring for detected/derived entries (not legal conclusions).

| Risk Category | Risk Description | Probability | Impact | Score | Trigger | Mitig resp |
|---|---|---|---|---|---|---|
| Tracking | Third-party tracking scripts were detected on public pages. Without region-appropriate consent configuration, regulatory exposure may increase. | **Likely (4)** | **Major (4)** | **16** | Google Analytics and Meta Pixel scripts detected in page source. | Review consent configuration for target regions. Ensure vendor disclosure matches deployed scripts. |
| Data capture | Customer-facing forms appear to collect personal information. Inadequate transparency or retention controls may increase compliance and operational risk. | **Possible (3)** | **Major (4)** | **12** | Contact and checkout forms detected with personal-data field signals (heuristic). | Audit form fields for minimum necessary data. Confirm storage, retention, and access controls. |

| Risk Category | Risk Description | Probability | Impact | Score | Trigger | Mitig resp |
|---|---|---|---|---|---|---|
| Accessibility | A portion of meaningful images were detected without alt text. This may affect accessibility depending on audience and jurisdiction. | **Possible (3)** | **Minor (2)** | **6** | 7 of 24 images missing alt text based on lightweight heuristic scan. | Add descriptive alt text to meaningful images on key product and conversion pages. |
| Compliance | No dedicated cookie policy page detected on standard public paths. | **Possible (3)** | **Moderate (3)** | **9** | Cookie policy not detected via homepage links or common public paths. | Publish and link a cookie policy page outlining tracking technologies and purposes. |

Note: Register scores reflect probability×impact per entry. The overall risk level is derived separately from the signal model.

# Findings by category

What was detected on the scanned surface (scope-locked).

## Connection

- HTTPS: Detected

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

## Policies (public-path detection)

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

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

## Cookies & tracking (HTML detection)

- Tracking scripts: Google Analytics, Meta Pixel
- Cookie vendor signals: OneTrust

Detections are based on observable HTML/script references. Interaction-gated or dynamically loaded tags may not be detected.

## Consent indicators (heuristic)

- Cookie/consent banner indicator: Detected

Heuristic signal based on text/DOM patterns and consent vendor markers. Not a guarantee.

## Forms & data capture (heuristic)

- Forms detected: 3
- Potential personal-data field signals: 2

Personal-data signals are heuristic counts based on common field names. They are not legal classifications.

## Accessibility signals (heuristic)

- Images missing alt text: 7 of 24
- Note: Several product images missing alt text.

Accessibility checks are lightweight and indicative only. A full audit typically requires broader coverage and manual testing.

## Contact & identity signals

- Contact/business identity signals: Detected

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

# Common next steps

General orientation only — not legal advice.

The items below are commonly reviewed when these signals appear. They're presented as practical next steps and are not prescriptive requirements.

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

# Methodology & limitations

How this snapshot is produced, and what it does not do.

## Methodology (this scan)

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

## Scope and exclusions

- No full-site crawling.
- Public, unauthenticated HTML only (no logins).
- No 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.

# Report verification

Public integrity check for this sealed snapshot.

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)

b50d49f57a066f6cc6274c743a896f6bea7c56f54d993c6f7848c6988eeb5319

## Verification link

/verify/b50d49f57a066f6cc6274c743a896f6bea7c56f54d993c6f7848c6988eeb5319

## 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)

Scan to verify