GETGDPRSCAN

GDPR Compliance Report

example-store.com

Good Compliance

COMPLIANCE SCORE

5
RECOMMENDED ACTIONS

2
HIGH PRIORITY

2
MEDIUM PRIORITY

"Session cookies set before consent; supervisory authority complaint right not mentioned in privacy policy"

Priority Actions

The site has solid technical foundations — consent-gated tracking, HTTPS, and proper form handling — but the privacy policy contains meaningful gaps including missing supervisory authority information, implied consent language, and incomplete data subject rights disclosures.

HIGH

Stop cookies from firing before consent is given

Audit your consent management setup to ensure no cookies — beyond strictly necessary session cookies — are placed on the visitor's device until they actively accept via the banner.

HIGH

Add right to complain to a data protection authority

Update your privacy policy to explicitly state that users have the right to file a complaint with their national data protection authority — this is a mandatory disclosure under Art. 13(2)(d) GDPR.

MEDIUM

Explicitly list all individual data subject rights

Add a dedicated section describing users' GDPR rights, including access, rectification, erasure, portability, restriction, and objection.

MEDIUM

Remove implied consent wording from privacy policy

The policy should not state that users automatically agree to it simply by using the website. Consent must be actively given.

LOW

Consider switching to a privacy-friendly analytics tool

Replacing behavioral analytics with a tool like Plausible or self-hosted Matomo would eliminate the need for analytics consent entirely, reducing compliance complexity.

Detailed Findings

Cookie & Consent

✓ **Cookie banner present**
A cookie consent banner is displayed to visitors.

✓ **Language preference cookie set before consent**
Language preference cookies are technically necessary for site functionality and do not require prior consent.

✓ **Session cookie set before consent**
Session cookies are strictly necessary for basic site operation (e.g., shopping cart, login) and are exempt from prior consent requirements.

✗ **Tracking or functional cookies loaded before consent**
Despite the banner, the scan detected cookies being set before the user has interacted with the consent mechanism, which violates GDPR's requirement for prior, freely given consent.

! **Consent mechanism exists and gates trackers**
Trackers appear to be blocked by the consent tool in principle, but the pre-consent cookie firing undermines the effectiveness of this gate.

Tracking & Analytics

! **Third-party tracking pixel detected**
A third-party tracking pixel is present; it appears consent-gated, but the consent mechanism must be verified to ensure it fires only after explicit opt-in.

! **Behavioral analytics script loaded**
An analytics script is loaded on the site; it should only activate after the user grants consent, as it tracks behavioral data.

✗ **Privacy-friendly analytics in use**
No privacy-friendly analytics tool (such as Plausible or self-hosted Matomo) is used; the active analytics services require consent and carry higher GDPR risk.

✓ **Consent-gating of third-party trackers**
The site uses a consent management approach intended to block third-party trackers until consent is given — a good practice that should be audited to confirm it works consistently.

Data Collection

✓ Low-sensitivity form (GET method, no personal data)

A search or filter-type form using GET collects no email, phone, or name data — low risk and no consent checkbox needed.

✓ High-sensitivity form (POST method, collects name and email)

The contact or newsletter form uses POST (correct for sensitive data) and collects name and email address.

✓ Consent checkbox on high-sensitivity form

The high-sensitivity form includes a consent checkbox — good practice that supports a valid legal basis for processing name and email.

Privacy Policy

✓ Privacy policy exists and is accessible

A publicly accessible privacy policy is available on the website.

✓ Data controller identity and contact details disclosed

The policy identifies the data controller and provides contact information.

✓ Processing purposes and legal basis stated (Art. 6 GDPR)

The policy explains the legal bases used for processing personal data, including consent and contractual necessity.

✓ Data recipients identified

The policy lists payment, hosting, analytics, and operational service providers involved in data processing.

✓ Data retention periods stated

Specific retention periods are defined for multiple categories of personal data.

! Data subject rights covered (Art. 15-21 GDPR)

Some GDPR rights are referenced, but access, portability, rectification, and erasure rights are not clearly listed individually.

! Right to withdraw consent mentioned

The policy references consent withdrawal, but does not clearly state users may withdraw consent at any time.

✗ Right to lodge a complaint with a supervisory authority

The policy does not mention the user's right to file a complaint with a data protection supervisory authority.

✗ Implied consent language

The policy implies that continued website use equals agreement, which is not valid GDPR consent.

! International data transfers and safeguards disclosed

International data transfers may occur, but the policy does not clearly explain the safeguards used.

Technical Security

✓ HTTPS enabled

The entire site is served over HTTPS, ensuring data in transit is encrypted.

✓ Sensitive form uses POST method

The form collecting personal data uses POST, preventing it from appearing in URLs or server logs.