

SYNTHETISCHER MUSTERBERICHT · Kein Kundensystem, kein Zertifikat.

PRÜFBERICHT · SICHERHEIT & COMPLIANCE

Wie sicher ist MAVENS-Demoshop?

MAVENS-Demoshop · geprüft am 21.09.2026 · 11:47 UTC · Commit efeed21d7586

Noch nicht freigabefähig.

3 Punkte müssen vor dem nächsten Release erledigt werden. Zusätzlich bleiben 4 Prüfverfahren unvollständig. Erst nach Behebung und erneuter Prüfung ist eine Freigabeaussage möglich. Die Zahl ausgeführter Einzelregeln wurde nicht gemessen; Katalogzahlen sind keine Sicherheitsquote.

GEPRÜFT ALS: ÖFFENTLICHE WEBSITE (EINSTIEG `index.html`) · TELEMEDIENPFLICHTEN GEPRÜFT

1.437 KRITERIEN IM KATALOG · AUSFÜHRUNGSUMFANG SIEHE PRÜFVERFAHREN

3 Sofort Vor dem nächsten Release bearbeiten	4 Zeitnah Zeitnah einplanen und nachprüfen	5 Ordnung Nachweise und Pflege einplanen
---	---	---

Wer erledigt das:

KI-Agent 5 x

Update & Release 0 x

Mensch entscheidet 7 x

PRÜFZEITPUNKT	21.09.2026 · 11:47 UTC
REGELWERK	2026.09.4/sme-eu-web
PRÜFPROFIL	commercial-v1
PRÜFWERKZEUG	MAVENS Core 0.10.0
COMMIT	efeed21d75868f5bef0ad252164f7e69c3b979ef
AUFTRAGS-ID	synthetic-771fb41b-c976-419b-9bad-d09c7253e633

Was geprüft wurde

4 Regelquellen mit 1.437 Kriterien im Katalog. Katalogzahlen belegen weder Anwendbarkeit noch Ausführung. Ausgeführte oder bestandene Einzelregeln wurden nicht gezählt. Eine Sicherheitsquote wird daraus nicht abgeleitet. Schwachstellen-Datenbanken (Trivy CVE-Datenbank): 0 Pakete mit bekannten Lücken. Datenbanken sind keine Kriterien und zählen nicht in die 1.437.

PRÜFVERFAHREN	ERGEBNIS	UMFANG
Zugangsdaten im Code	ohne Befund	3 Dateien geprüft; 0 nicht ausgewertet
Datenbank-Migrationen	ohne Befund	1 Migrationsdateien geprüft; 0 nicht ausgewertet
Mandantentrennung, statisch (RLS)	Befund	1 tables tracked; RLS without policies defaults to deny; effective access not tested
Datenbankkonfiguration, live (RLS)	übersprungen	database assurance requires a separate authorized evidence context; source snapshot scans never connect to a database
Abhängigkeiten (pnpm audit)	nicht verfügbar	trusted package-manager audit currently supports pnpm lockfiles only
Personenbezogene Daten in Logs	Befund	1 von 1 Quelldateien geprüft
Anmeldung & Sessions	ohne Befund	1 anmelderelevante Dateien geprüft (statische Heuristik)
DSGVO · Einwilligung	Befund	Verarbeitungsverzeichnis fehlt, 0 Tracking-Dateien ohne Einwilligungsschranke
DSGVO · Art. 32 Nachweise	Befund	kein Verarbeitungsverzeichnis; Art.-32-Erklärungen geprüft; Wirksamkeit im Betrieb nicht nachgewiesen
CRA-Bereitschaft	Befund	Meldeweg, Offenlegung, Support- und Patch-Policy geprüft
Software-Lieferkette	Befund	0 Lockfile(s), 0 Workflow(s), Lizenz- und Auslieferungs-Erklärungen geprüft; Wirksamkeit im Betrieb nicht nachgewiesen
Zugangsdaten (Gitleaks)	ohne Befund	gitleaks mit gebundener Konfiguration abgeschlossen Werkzeug 8.30.1. Git-Historie: nicht geprüft.
Statische Codeanalyse (Semgrep)	Befund	semgrep mit gebundener Konfiguration abgeschlossen Werkzeug 1.176.0. 7 Regeln konfiguriert. 1 Dateien geprüft.
Abhängigkeiten (Trivy CVE)	Fehler	trusted scanner returned invalid or incomplete evidence; raw diagnostic withheld
Infrastruktur-Konfiguration (Trivy)	Fehler	trusted scanner returned invalid or incomplete evidence; raw diagnostic withheld
Live-Header des Servers	nicht anwendbar	keine deployment_url im Prüfprofil: kein Server wurde kontaktiert
Vertrauenswürdigkeit der Pakete	nicht anwendbar	keine package.json
Schutz-Header	nicht anwendbar	keine package.json: keine Webanwendung

PRÜFVERFAHREN	ERGEBNIS	UMFANG
Datei-Uploads	nicht anwendbar	kein Upload-Handler in 1 Quelldateien gefunden: dieser Quellstand nimmt keine Dateien entgegen
KI-Verordnung	nicht anwendbar	kein Model-SDK, kein Modell-Endpunkt, kein KI-System-Manifest im Code gefunden; die KI-Verordnung (EU) 2024/1689 greift für diesen Quellstand nicht
Website-Pflichten	Befund	öffentliche Website erkannt (index.html); 1 Seiten und 2 Quelldateien geprüft: Impressum fehlt, Datenschutzerklärung fehlt, 0 Dateien mit Drittanbieter-Einbettung ohne Einwilligung, Consent-Mechanismus fehlt

Was dieser Lauf nicht prüft

Laufzeit und Angriffe: Alles basiert auf dem Quellcode. Kein Penetrationstest, keine Beobachtung des laufenden Systems. „Ohne Befund“ heißt: kein Muster im Code - nicht: unangreifbar.

Offene Prüfverfahren: Datenbankkonfiguration, live (RLS) (übersprungen); Abhängigkeiten (pnpm audit) (nicht verfügbar); Abhängigkeiten (Trivy CVE) (Fehler); Infrastruktur-Konfiguration (Trivy) (Fehler). Diese Verfahren gelten nicht als bestanden.

Nicht anwendbare Verfahren: Die Gründe stehen bei den jeweiligen Verfahren. Diese Ergebnisse sind kein Nachweis einer ausgeführten Sicherheitsprüfung.

Rechtlicher Kontext: Betreiber-, Markt- und Verarbeitungskontext stehen nicht im Code. Die Fragen im regulatorischen Abschnitt klären, ob und wie die Instrumente gelten.

Was gefunden wurde

15 Einzeltreffer, nach Ursache zu 12 Aufgaben zusammengefasst. Risikoklassen: 9 Blocker · 6 Hoch. Jede einzelne Fundstelle mit Befund-ID steht im gespeicherten Prüfergebnis; dessen Prüfsumme steht unter „Nachweis & Geltung“.

AUFGABE	WANN	WER	UMFANG
A01 · Datenschutzerklärung anlegen und im Footer jeder Seite verlinken	Sofort	Mensch entscheidet	1 Stelle
A02 · Impressum anlegen und im Footer jeder Seite verlinken – die Angaben liefert der Betreiber	Sofort	Mensch entscheidet	1 Stelle
A03 · Tabelle ohne Mandantentrennung absichern	Sofort	KI-Agent	1 Stelle
A04 · Reproduzierbaren Build und Inventar sicherstellen	Zeitnah	KI-Agent	3 Stellen · 3 Dateien
A05 · Dynamische Codeausführung mit eval prüfen	Zeitnah	KI-Agent	1 Stelle
A06 · Personenbezogene Daten aus Logs und Browser fernhalten	Zeitnah	KI-Agent	1 Stelle
A07 · TLS-Zertifikatsprüfung wieder aktivieren	Zeitnah	KI-Agent	1 Stelle
A08 · Meldeweg und Support-Policy dokumentieren	Ordnung	Mensch entscheidet	2 Stellen · 2 Dateien
A09 · Lieferketten-Erklärung anlegen	Ordnung	Mensch entscheidet	1 Stelle
A10 · Verarbeitungsinventar vervollständigen	Ordnung	Mensch entscheidet	1 Stelle
A11 · Verarbeitungsverzeichnis anlegen	Ordnung	Mensch entscheidet	1 Stelle
A12 · Verschlüsselungs-Nachweis dokumentieren	Ordnung	Mensch entscheidet	1 Stelle

Was das regulatorisch bedeutet

Der Scan prüft im Code, was sich dort prüfen lässt: technische Schutzmaßnahmen und das Vorhandensein der geforderten Nachweise. Ob ein Instrument für den Betreiber gilt, ergibt sich nicht aus dem Code.

INSTRUMENT	ERGEBNIS	PFLICHTEN	AUFGABEN
DSGVO	Befund	4 von 6 mit Befund, 1 nicht prüfbar	A03 A05 A06 A07 A10 A11 A12

INSTRUMENT	ERGEBNIS	PFLICHTEN	AUFGABEN
Cyber Resilience Act	Befund	2 von 4 mit Befund, 1 nicht prüfbar	A04 A08 A09
KI-Verordnung (AI Act)	nicht anwendbar	kein Model-SDK, kein Modell-Endpunkt, kein KI-System-Manifest im Code gefunden; die KI-Verordnung (EU) 2024/1689 greift für diesen Quellstand nicht	-
Website-Pflichten (DDG, TDDDG)	Befund	2 von 5 mit Befund	A01 A02

Diese Fragen beantwortet kein Scan, sondern der Betreiber:

DSGVO: (1) Werden personenbezogene Daten von EU-Bürgern verarbeitet, und in welcher Rolle (Verantwortlicher oder Auftragsverarbeiter)? (2) Gibt es ein Verarbeitungsverzeichnis außerhalb des Repositories? (3) Werden Daten an Dienstleister außerhalb der EU übertragen?

Cyber Resilience Act: (1) Wird das Produkt in der EU in Verkehr gebracht, und in welcher Rolle (Hersteller, Importeur, Händler)? (2) Ab wann und wie lange gilt der zugesagte Support-Zeitraum? (3) Existiert ein Meldeweg für Schwachstellen außerhalb des Repositories?

KI-Verordnung (AI Act): (1) Setzt das Produkt KI ein, die außerhalb dieses Codes liegt (z. B. angebundene Agenten oder externe Modelle)? (2) Trifft das System Entscheidungen mit Wirkung auf Personen (Anhang III)? (3) In welcher Rolle: Anbieter oder Betreiber?

Website-Pflichten (DDG, TDDDG): (1) Ist die Website geschäftlich, also nicht rein privat oder familiär genutzt? (2) Wer ist der Betreiber, und stehen seine Angaben (Anschrift, Kontakt, Vertretung, Register) bereit? (3) Werden Besucher gemessen oder Inhalte Dritter eingebunden, und wurde dafür eine Einwilligung vorgesehen?

Was jetzt zu tun ist

Jede Aufgabe nennt, was passiert, wenn man sie liegen lässt, wer sie erledigen kann und woran die Erledigung erkennbar ist.

SOFORT

Vor dem nächsten Release bearbeiten. Die Priorität folgt dem Regelwerk; die Problemart steht an jeder Aufgabe.

A01 · Datenschutzerklärung anlegen und im Footer jeder Seite verlinken

1 Stelle

Mensch entscheidet

Problemart: Rechtliche Anforderung

Die Website hat keine Datenschutzerklärung. Sobald Besucher die Seite aufrufen, werden Daten verarbeitet; darüber muss informiert werden.

Behebung: Seite /datenschutz anlegen und im Footer jeder Seite verlinken. Inhalt nach Art. 13 DSGVO: Verantwortlicher, Zwecke und Rechtsgrundlagen, Empfänger (Hosting, Mailversand, Analyse), Speicherdauer, Betroffenenrechte. Die Angaben liefert der Betreiber; der Agent baut die Seite.

Erledigt, wenn: Der Betreiber hat Anwendbarkeit, Angaben und Vollständigkeit geprüft. Erforderliche Seiten sind ohne Platzhalter erreichbar und von den betroffenen Seiten verlinkt; Linkprüfung und erneuter Scan sind dokumentiert. Ein Scan ersetzt diese inhaltliche Prüfung nicht.

`index.html`

A02 · Impressum anlegen und im Footer jeder Seite verlinken - die Angaben liefert der Betreiber

1 Stelle

Mensch entscheidet

Problemart: Rechtliche Anforderung

Die Website hat kein Impressum. In Deutschland ist das Pflicht für praktisch jede geschäftliche Website und der häufigste Abmahngrund.

Behebung: Seite /impressum anlegen und im Footer jeder Seite verlinken. Angaben nach DDG § 5: Name und Anschrift, E-Mail und ein zweiter schneller Kontaktweg, Vertretungsberechtigte, Register und Registernummer, USt-IdNr. sofern vorhanden. Die Angaben liefert der Betreiber; der Agent baut die Seite.

Erledigt, wenn: Der Betreiber hat Anwendbarkeit, Angaben und Vollständigkeit geprüft. Erforderliche Seiten sind ohne Platzhalter erreichbar und von den betroffenen Seiten verlinkt; Linkprüfung und erneuter Scan sind dokumentiert. Ein Scan ersetzt diese inhaltliche Prüfung nicht.

`index.html`

A03 · Tabelle ohne Mandantentrennung absichern

1 Stelle

KI-Agent

Problemart: Technische Sicherheit

Eine Datentabelle ist nicht durch Mandantenzugriff geschützt - Kunden könnten Daten anderer Kunden sehen.

Behebung: ALTER TABLE ... ENABLE ROW LEVEL SECURITY; Force RLS; Policy mit account_id-Filter ergänzen.

Erledigt, wenn: In einer Testumgebung sind eigene Zugriffe erlaubt und fremde Mandanten sowie anonyme Zugriffe gemäß Sollberechtigung abgewiesen. Positive und negative Tests für Lesen und Schreiben sowie erneute Prüfung der Migration sind dokumentiert.

`Table ["public","orders"] has RLS disabled in reconstructed migrations; exposure depends on grants and roles`

ZEITNAH Zeitnah einplanen und nachprüfen. Die Priorität allein belegt keine Ausnutzbarkeit.

A04 · Reproduzierbaren Build und Inventar sicherstellen

3 Stellen · 3 Dateien

KI-Agent

Problemart: Technische Sicherheit

Der ausgelieferte Softwarestand ist nicht reproduzierbar oder seine Bestandteile sind nicht vollständig inventarisiert.

Behebung: Lockfile-Build erzwingen, Delivery-Workflow und Lizenzinventar ergänzen.

Erledigt, wenn: Die betroffenen Build-, Inventar- oder Lieferketten-Nachweise sind am aktuellen Quellstand geprüft. Ein frischer Build und erneuter Scan sind dokumentiert; fehlende organisatorische Angaben sind vom Betreiber bestätigt.

```
no supported dependency lockfile exists
.github/workflows
compliance/third-party-licenses.json
```

A05 · Dynamische Codeausführung mit eval prüfen

1 Stelle

KI-Agent

Problemart: Technische Sicherheit

Die Regel erkennt einen nicht konstanten Wert in eval. Ungeprüfte Eingaben können dadurch als Code ausgeführt werden.

Behebung: Dynamische Codeausführung entfernen oder den Datenfluss so korrigieren, dass externe Eingaben nicht als Code interpretiert werden.

Erledigt, wenn: Manipulierte Testeingaben werden als Daten behandelt oder abgewiesen; die vorgesehene Funktion arbeitet weiter. Datenflusstest und erneuter Scan sind dokumentiert.

```
app.js:3
```

A06 · Personenbezogene Daten aus Logs und Browser fernhalten

1 Stelle

KI-Agent

Problemart: Technische Sicherheit

Personenbezogene Daten könnten in Protokolle oder den Browser gelangen - das darf nicht passieren.

Behebung: PII nicht loggen (console.log/logger) und nicht an Client-Komponenten ('use client') übergeben.

Erledigt, wenn: Tests mit synthetischen personenbezogenen Daten belegen die Entfernung oder Maskierung in Logs und Browserausgaben. Benötigte Diagnoseinformationen bleiben nutzbar; erneuter Scan und geprüfte Ausgaben sind dokumentiert.

```
app.js:7
```

A07 · TLS-Zertifikatsprüfung wieder aktivieren

1 Stelle

KI-Agent

Problemart: Technische Sicherheit

Die Regel erkennt eine deaktiverte TLS-Zertifikatsprüfung. Die Identität der Gegenstelle könnte ungeprüft bleiben.

Behebung: Zertifikatsprüfung aktivieren und erforderliche Vertrauensanker gezielt konfigurieren.

Erledigt, wenn: Eine gültige Testgegenstelle wird akzeptiert, ein ungültiges Zertifikat abgewiesen. Beide Tests und erneuter Scan sind dokumentiert.

```
app.js:5
```

ORDNUNG Nachweise und Pflegeaufgaben einplanen. Das Ergebnis der Nachprüfung bleibt offen.

A08 · Meldeweg und Support-Policy dokumentieren

2 Stellen · 2 Dateien

Mensch entscheidet

Problemart: Dokumentation / Nachweis

Sicherheitsmeldungen, Patchfristen oder der Supportzeitraum sind nicht verbindlich geregelt.

Behebung: SECURITY.md und compliance/support-policy.yaml mit Intake, Disclosure, Supportende und Patch-SLAs pflegen.

Erledigt, wenn: Die zuständige Person hat Anwendbarkeit und geforderte Angaben geprüft. Nachweis und tatsächlicher Prozess sind abgeglichen; offene Kontextfragen sind beantwortet. Erneuter Scan und fachliche Prüfung sind dokumentiert, ohne daraus eine Rechtskonformität abzuleiten.

SECURITY.md
compliance/support-policy.yaml

A09 · Lieferketten-Erklärung anlegen

1 Stelle

Mensch entscheidet

Problemart: Dokumentation / Nachweis

Die Erklärung zu Lieferketten-Kontrollen fehlt. Das heißt nicht, dass die Kontrollen fehlen - nur, dass sie nicht belegt sind.

Behebung: Builder-Identität, geschützte Branches und OIDC-basierte kurzlebige Least-Privilege-Credentials deklarieren.

Erledigt, wenn: Die betroffenen Build-, Inventar- oder Lieferketten-Nachweise sind am aktuellen Quellstand geprüft. Ein frischer Build und erneuter Scan sind dokumentiert; fehlende organisatorische Angaben sind vom Betreiber bestätigt.

.maestro/supply-chain.yaml

A10 · Verarbeitungsinventar vervollständigen

1 Stelle

Mensch entscheidet

Problemart: Dokumentation / Nachweis

Der geforderte Nachweis fehlt oder ist unvollständig. Das heißt nicht, dass die Maßnahme im Betrieb fehlt - nur, dass sie nicht belegt ist.

Behebung: compliance/processing-manifest.yaml vollständig und maschinenlesbar pflegen.

Erledigt, wenn: Die zuständige Person hat Anwendbarkeit und geforderte Angaben geprüft. Nachweis und tatsächlicher Prozess sind abgeglichen; offene Kontextfragen sind beantwortet. Erneuter Scan und fachliche Prüfung sind dokumentiert, ohne daraus eine Rechtskonformität abzuleiten.

processing manifest is missing

A11 · Verarbeitungsverzeichnis anlegen

1 Stelle

Mensch entscheidet

Problemart: Dokumentation / Nachweis

Es ist nicht dokumentiert, welche personenbezogenen Daten warum verarbeitet werden - DSGVO-Grundpflicht.

Behebung: processing_manifest.yaml anlegen: pro Datenkategorie Zweck, legal_basis, retention, PII-Felder.

Erledigt, wenn: Die zuständige Person hat Anwendbarkeit und geforderte Angaben geprüft. Nachweis und tatsächlicher Prozess sind abgeglichen; offene Kontextfragen sind beantwortet. Erneuter Scan und fachliche Prüfung sind dokumentiert, ohne daraus eine Rechtskonformität abzuleiten.

processing_manifest.yaml fehlt - Datenverarbeitungszwecke und Rechtsgrundlagen sind nicht maschinenlesbar dokumentiert

A12 · Verschlüsselungs-Nachweis dokumentieren

1 Stelle

Mensch entscheidet

Problemart: Dokumentation / Nachweis

Der Nachweis zur Verschlüsselung fehlt oder ist ungültig. Das heißt nicht, dass die Verschlüsselung fehlt - nur, dass sie nicht belegt ist.

Behebung: TLS 1.2+ und die At-Rest-Verschlüsselung in compliance/security-controls.yaml dokumentieren und technisch erzwingen.

Erledigt, wenn: Die zuständige Person hat Anwendbarkeit und geforderte Angaben geprüft. Nachweis und tatsächlicher Prozess sind abgeglichen; offene Kontextfragen sind beantwortet. Erneuter Scan und fachliche Prüfung sind dokumentiert, ohne daraus eine Rechtskonformität abzuleiten.

compliance/security-controls.yaml

Hilfe beim Umsetzen: 30 Minuten mit dem MAVENS-Team, kostenlos. mavens.de/contact

Nachweis & Geltung

Prüfverfahren: Automatisierte, regelbasierte Analyse des angegebenen Quellstands. Der Bericht übernimmt das gespeicherte Scannerurteil; kein Sprachmodell bewertet Befunde beim Versand neu.

Geltungsbereich: Die Aussage gilt für das benannte Repository und den vollständigen Commit. Test-, Fixture- und Designdateien werden gezählt, aber nicht als Aufgabe geführt. Eine spätere Code-Version ist nicht Gegenstand dieses Berichts.

Bewertung und Grenzen: Keine Zertifizierung, keine Rechtsberatung, kein manueller Penetrationstest. Organisatorische Maßnahmen, die Wirksamkeit von Korrekturen und nicht ausgeführte Prüfschritte sind nicht nachgewiesen.

Einzelbefunde: Dieses Protokoll fasst zusammen. Jede Fundstelle mit Befund-ID, Schweregrad und Hinweis steht unverändert im gespeicherten Prüfergebnis, das die folgende SHA-256-Prüfsumme bezeichnet; sie ist keine digitale Signatur dieses PDFs.

Technische Referenzen

Vorlage	mavens-assurance-report / 2.2
Auftrags-ID	synthetic-771fb41b-c976-419b-9bad-d09c7253e633
Repository	MAVENS-Demoshop
Commit	efeed21d75868f5bef0ad252164f7e69c3b979ef
Tree-SHA	7fe64476a7aed87dc4b244233b44c7729c6d1663
Quellstand-Digest	sha256:c8f92c71acbd5cb625115cb40a8244c017dbcf9109a5dc65ae18c61b4e657bf
Prüfprofil	commercial-v1
Regelwerk	2026.09.4/sme-eu-web
Ausführungsumgebung	local native tools; packaged trusted policy; no application execution; not a production runner job
Textbericht SHA-256	sha256:96956474677a942af1d442fa7f071d966f2796bff196df5e2e39527e48e23359
Einzeltreffer	15 gesamt · 15 blockierend · 4 Prüfausfälle
Core-Version	0.10.0
Core-Paket SHA-256	sha256:b51529fd9b555b6c274aaa5297ed10b8b6b5c8286e0fb6848f9e7bfcecb0cb61
Konfiguration: Zugangsdaten (Gitleaks)	sha256:642fca5b933cbaf3a07a37339df426bb189a5875fe8dfe4c627e202d6510c636
Konfiguration: Statische Codeanalyse (Semgrep)	sha256:1f807dca7ae3dbe614e938f104914aa043de81c53ee72cf1b8c2a5f6258368f6