

# Checkliste: SEO & Sicherheit

## 1. Sicherheits-Header prüfen & setzen

### X-Content-Type-Options vorhanden?

Header setzen: X-Content-Type-Options: nosniff

### X-Frame-Options gesetzt?

Verwendung von SAMEORIGIN empfohlen

### Content-Security-Policy vorhanden?

Mindestens: default-src 'self'; weitere Quellen gezielt freigeben

### Referrer-Policy aktiv?

Empfehlung: strict-origin-when-cross-origin

### HSTS gesetzt?

Header setzen: Strict-Transport-Security mit max-age & includeSubDomains

## 2. Mixed Content & Ressourcen absichern

### Lädt die Seite alle Ressourcen per HTTPS?

Keine HTTP-Ressourcen auf HTTPS-Seiten einbinden

### Externe Inhalte mit Subresource Integrity?

Nutze integrity-Attribut für JS/CSS von Drittanbietern

### Noch HTTP-Links intern/extern vorhanden?

Alle Links auf https:// umstellen, wenn möglich

### Skripte von vertrauenswürdigen Quellen?

Nur geprüfte und nötige Drittanbieter-Ressourcen laden

### Content-Security-Policy einschränkend gesetzt?

Ressourcenquellen gezielt über CSP einschränken

### 3. Formulare & Datenübertragung

#### **Formulare nur über HTTPS?**

Seite und Form-Action müssen HTTPS nutzen

#### **Warnungen im Browser?**

Mixed Content oder unsichere Formulare vermeiden

#### **Keine sensiblen Daten im Referrer?**

Referrer-Policy entsprechend setzen

#### **Google reCAPTCHA korrekt eingebunden?**

Immer über HTTPS laden, CSP-Regeln beachten

#### **Externe Formular-Services nutzen HTTPS?**

Anbieter prüfen und nur verschlüsselt einbinden

### 4. Sichere Linkstruktur

#### **Externe Links mit target='\_blank' abgesichert?**

Immer rel='noopener noreferrer' verwenden

#### **HTTP auf HTTPS weitergeleitet?**

301-Redirects für alle HTTP-Aufrufe einrichten

#### **Canonical-Tags auf HTTPS?**

Canonical-URLs immer in HTTPS-Version

#### **Sitemap mit HTTPS-URLs?**

Nur HTTPS-Links in der XML-Sitemap verwenden

#### **Links mit target='\_blank' abgesichert?**

Vermeide Reverse Tabnabbing durch rel='noopener' oder 'noreferrer'