Trusted Heroes

Prüfsiegel für Online Shops und Websites

Detaillierter Prüfkatalog zur Evaluierung von Online Shops und Webseiten

www.trusted-heroes.com

info@trusted-heroes.com

Inhaltsverzeichnis

Disclaimer

Der Einfachheit halber verwenden wir im Folgenden stets die männliche/abstrahierte Version von Nomen. Damit möchten wir keine Gruppen ausschließen oder benachteiligen. Von jeglicher Diskriminierung distanzieren wir uns.
Wenn im Verlauf des Prüfplans von Ware/Produkt oder Dienstleistung gesprochen wird, kann sich dies auch auf mehrere Produkte oder Dienstleistungen beziehen. Auch hier verzichten wir der Einfachheit halber auf weitere Plural-Nennungen.

Sollten Sie Fehler entdecken, Verbesserungen vorschlagen oder Fragen zu bestimmten Punkten haben, können Sie sich jederzeit bei Trusted Heroes melden.

E-Mail: info@trusted-heroes.com

1. Worum geht es in dem Prüfplan?

Damit eine Website oder ein Online Shop ein Trusted Heroes Gütesiegel erhält, muss es bestimmte Kriterien erfüllen. Der Prüfplan soll diese für Webseiten und Online Shops näher beschreiben, um die Prüfung für alle nachvollziehbar aufzubereiten.
Manche Kriterien sind essenziell, andere wichtig und wiederrum andere ein Nice to have. Dafür haben wir eine Ampel in den Farben ● Rot (Essenziell), ● Orange (Wichtig) und ● Grün (Nice to have). Kategorien, die für Webseiten nicht relevant sind, werden mit ● Blau (Nicht Webseiten-relevant) angezeigt.

Jeder von uns geprüfte Online Shop oder Website erhält einen Prüfbericht, in dem die hier festgelegten Kategorien abgearbeitet werden, um dementsprechend sagen zu können, ob die Domain die Prüfung bestanden hat und somit Trusted Heroes zertifiziert oder durchgefallen ist. Im Falle eines nicht Bestehens erhält die Seite keinen Trusted Heroes – Badge, welches bei bestandenen Shops/Websites entweder unten rechts zu finden ist und/oder in der Fußzeile (Footer) oder im oberen Header-Bereich eingebunden werden kann.

Nachfolgend sollen die Kriterien näher beschrieben werden und dargelegt werden, was wir bei den einzelnen Punkten im Detail überprüfen.

2. Prüfkategorien

2.1 Identitätscheck des Unternehmens

Ein Unternehmen sollte seine Identität offen darlegen und deutliche Angaben machen. Daher überprüfen wir zunächst den Hauptsitz des Unternehmens, da manche Länder keine Impressumspflicht haben. Für diese überprüfen wir dennoch Transparenzangaben zu Name, Anschrift, E-Mail-Adresse und Telefonnummer (keine Mehrwertnummer), da diese ein wichtiges Vertrauensmerkmal zur Echtheit sind.
Hierzu gehören neben dem **Namen** der betreffen Seite oder des Online Shops auch die **Anschrift**, **E-Mail-Adresse** und **Telefonnummer** (keine Mehrwertnummer) und im

Falle eines Online Shops auch die Handelsregisternummer, sofern die **Rechtsform** und Größe des Unternehmens das vorschreiben. Diese Informationen sollen leicht auffindbar sein, beispielsweise über einen Link zum Impressum oder zur Kontakt-Seite. Um die Echtheit des Shops zu überprüfen, vergleichen wir die Angaben im Impressum mit denen bei Crefo und ggf. auch über Northdata.

Prüfung auf	Beschreibung	Relevanz
Hauptsitz des Unternehmens	Fundament für Seriosität und Rechtskraft	●
Name, Anschrift, Kontakt	Pflichtangaben des Impressums	●
Handelsregistereintragung	Bei eintragungspflichtigen Rechtsformen erforderlich	● ●

Der Hauptsitz des Unternehmens ist relevant, um die Seriosität und Identität zu prüfen. Über den Hauptsitz kann geprüft werden, ob die Adresse wirklich existiert und damit eher ein Fake-Shop ausgemacht werden. Weiterhin lassen sich Punkte wie Datenschutz, AGB, Zahlungsabwicklungen und das Impressum über den Hauptsitz konkreter prüfen.

Der Hauptsitz des Unternehmens ist ein zentrales Kriterium, um die Identität und Seriosität zu prüfen. Über die Adresse lässt sich feststellen, ob das Unternehmen tatsächlich existiert. In den DACH-Ländern (Deutschland, Österreich, Schweiz) besteht eine gesetzliche Impressumspflicht (§ 5 DDG in Deutschland, § 5 ECG in Österreich und Art. 3 im UWG in der Schweiz). Pflichtangaben sind **Name oder Firma, Anschrift und Kontaktdaten**. Juristische Personen müssen zusätzlich ihre **Rechtsform** und den **Vertretungsberechtigten** nennen. Ein **Handelsregistereintrag** ist für Kapitalgesellschaften vorgeschrieben, nicht jedoch für Einzelunternehmer oder Kleingewerbe. Auch Eintragungen ins Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister mit entsprechender Registernummer können angegeben sein. Soweit vorhanden, können weitere Angaben wie **Umsatzsteuer-Identifikationsnummer** oder **Stammkapital** im Impressum aufgeführt sein. Wenn Angaben zum Kapital der Gesellschaft gemacht werden, muss auch das Stamm- und Grundkapital und der Gesamtbetrag der ausstehenden Einlagen, sofern noch nicht

alle gezahlt wurden, mit aufgeführt sein. Bei erlaubnispflichtigen Dienstleistungen ist zudem die zuständige **Aufsichtsbehörde** anzugeben. Zur Vermeidung von Betrug wird das Impressum mit offiziellen Registern und den **Domaininhaber**-Daten abgeglichen, da viele Fake-Shops unvollständige oder gefälschte Impressumsangaben verwenden.

2.2 Technische Sicherheiten

Die Sicherheit einer Seite ist äußert wichtig, um sensible Daten vom Unternehmen und der User zu schützen. Suchmaschinen legen großen Wert auf die Sicherheit und markieren Seiten ohne Verschlüsselung als unsicher.

Für die technische Sicherheit betrachten wir folgende Punkte:

Prüfung auf	Beschreibung	Relevanz
SSL/TLS-Verschlüsselung	Prüfung auf HTTPS	●
Verschlüsselungsstärke	Niveau des Verschlüsselungsschutzes	●
Content Security Policy	Richtlinie gegen Schadcode und Cross-Site-Scripting	●

2.2.1 SSL / TLS Verschlüsselung

Eine technisch sichere Seite wird heute über **TLS (Transport Layer Security)** verschlüsselt. TLS ist der Nachfolger des früher verwendeten **SSL** (Secure Sockets Layer) und gilt als aktueller Sicherheitsstandard.
Mit einem TLS-Zertifikat werden Daten wie persönliche Informationen oder Zahlungsdetails verschlüsselt und können nicht einfach von Dritten abgefangen werden.
Erkennbar ist die Verschlüsselung an der URL: sichere Seiten beginnen mit **https://** – das „S“ steht für „Secure“. Fehlt die Verschlüsselung, läuft die Seite nur über http://. Dies gilt bei Suchmaschinen als unsicher und ist nicht DSGVO-konform.

Weiterhin kann der HTTP-Header **HSTS** (HTTP Strict Transport Security) eingebaut werden, der den Browser dazu zwingt, immer auf die sichere https-Variante umzuleiten, um zu verhindern, dass ein User versehentlich auf einer unsichere http-Variante einsteigt.

2.2.2 Verschlüsselungsstärke

Man spricht von einer starken Verschlüsselungsstärke bei einer symmetrischen Verschlüsselung (AES – Advanced Encryption Standard) ab 128 Bit und bei einer asymmetrischen Verschlüsselung (RSA – Rivest Shamir Adleman, ECC – Ecliptic Curve Cryptography) ab 2048 Bit bei RSA und 265 Bit bei ECC:

- **AES-128 Bit**: gilt noch als sicher
- **AES-256 Bit**: stark und empfohlen und heutiger Standard
- **RSA**: 2048, 3072 bis 4096 Bit sicher | 1024 Bit ist unsicher!
- **ECC**: 256 Bit ist sicher (entspricht ungefähr 3072 Bit RSA)

Weiterhin als **unsicher** gelten **SHA-1** Verschlüsselungen, da sie kollisionsanfällig sind.

Folgend eine Liste mit weiteren gängigen Verschlüsselungsstärken:

Symmetrische:

- **3DES** (Triple DES): veraltet und nicht mehr empfohlen
- **Twofish**: sehr sicher bis 256 Bit aber selten zu sehen
- **Blowfish**: Vorgänger von Twofish bis max. 448 Bit, gilt als sicher, ist aber nicht modern
- **ChaCha 2.0**: moderne Alternative zu AES, oft in mobilen Anwendungen. 256 Bit gilt als sehr stark

Asymmetrische:

- **ElGamal**: Ähnlich wie RSA, aber kaum genutzt
- **DSA**: (Digital Signature Algorithm): Bei mehr als 2048 Bit – kaum genutzt

Hash-Verfahren:

- **SHA-256** / **SHA-3**: Stark
- **SHA-1** / **MD5**: Unsicher

Wir prüfen, welche Verschlüsselungsstärke vorherrscht, da diese für den Schutz der Seite als auch den User wichtig ist. Sollte uns auffallen, dass der Schutz veraltet oder ungenügend ist, sollte schnell geupgradet werden.

2.2.3 Content Security Policy

Die Content Security Policy (CSP) ist ein sehr relevanter Teil der technischen Sicherheit, da sie vor Cross-Site-Scripting und somit Datenklau schützen. Die CSP verhindert, dass Angreifer über manipulierte Inhalte oder unsichere Einbindungen schädlichen Code auf der Seite ausführen können. Daher sollte ein CSP-Header im HTTP-Response vorhanden sein. Der CSP kann hierbei verschiedene Direktiven haben:

- **default-src ‚self'**: Akzeptiert nur Inhalte der eigenen Domain
- **script-src**: Nur Skripte von definierten Quellen
- **object-src ‚none'**: Verhindert alte, unsichere Plugins wie Flash
- **report-uri** / **report-to**: Verstöße werden gemeldet

CSP ist besonders bei Online Shops wichtig, da hier wichtige Kundendaten fließen. Auch bei normalen Websites, die rein informativer Natur sind, ist eine CSP sinnvoll, das Fehlen einer solchen ist jedoch weniger gravierend.

2.3 Klarheit & Transparenzen

User müssen gut geschützt sein, um sicher auf dem Online Shop oder der Website navigieren zu können, damit sie in keine Preisfallen oder Ähnliches tappen.
Daher arbeiten wir in unserer Prüfung mehrere Punkte ab, die für Besucher schnell ersichtlich sein sollten, um ihnen Sicherheit liefern zu können.
Dazu gehören folgende Aspekte, die dann im Anschluss näher beleuchtet werden:

Prüfung auf	Beschreibung	Relevanz
Produktangebot	Klare Produkt-Vorstellung	● ●
Preistransparenz	Offene Darlegung aller anfallenden Kosten	● ●

Zahlungsanbieter	Sind seriöse Zahlungsanbieter für den Bezahlvorgang angeboten?	● ●
Transparenz über Drittanbieter	Dritte müssen erkennbar gemacht werden	● ●
Angaben der Lieferzeiten	Angaben der Lieferzeit in verschiedene Länder und informieren über Lieferprobleme	● ●
Bestellprozess und -bestätigung	Vollständige Übersicht vor und nach Abschluss einer Bestellung	● ●

2.3.1 Produktangebot

Die angebotenen Produkte (fortfolgend nur noch als Produkte bezeichnet) dürfen keiner unserer **Ausgeschlossenen Produktkategorien** entsprechen. Hierzu gehören beispielsweise illegale Produkte wie Waffen oder Drogen, Produkte, die Mensch, Umwelt oder Tier Schaden zufügen könnten oder solche, die diskriminierend sind. Werden Produkte angeboten, die erst ab 18 Jahren veräußert werden dürfen (Alkohol- oder nikotinhaltige Produkte), so muss eine **Altersabfrage** bei Betreten der Seite erfolgen.

Bei den angebotenen Produkten muss klar erkennbar sein, ob es sich um **B2B oder B2C** handelt. Das Produkt muss vollständig und eindeutig beschrieben sein, indem sowohl die **Herstellerinformationen** auf der Produktdetailseite auffindbar sind – vor allem wenn der Shopbetreiber nicht der Hersteller ist – als auch alle relevanten **Eigenschaften** und **Sicherheitshinweise** angegeben sind. Bei Waren sollte auf das gesetzliche Mängelhaftungsrecht hingewiesen werden.
Außerdem muss ersichtlich sein, ob es sich um einen einmaligen Preis oder ein **Abo-Modell-Produkt** handelt. Bei letzterem muss neben **Vertragsdauer** auch auf eine **Kündigungsmöglichkeit** hingewiesen werden.
Bei **digitalen Produkten** werden Funktionsweise zusammen mit technischen Schutzmaßnahmen sowie Interoperabilität / Kompatibilität angegeben.
Ein Produkt darf **kostenpflichtige Zusatzleistungen nicht vorausgewählt** werden, sofern dies nicht im Voraus vereinbart war.

2.3.2 Preistransparenz

Käufer sollten über alle anfallenden Kosten informiert werden. Dazu gehören

- Grundpreis der Ware nach Gewicht, Volumen, Länge, Fläche oder sonstiges?
- Anfallende Steuern (Mehrwertsteuer, Umsatzsteuer)
- Abgaben
- Versandkosten
- Sonstige Zusatzkosten
- Bei Abomodellen: Preis im Intervall
- Gesamtpreis (außer es kann im Voraus nicht angegeben werden, dann ist die Angabe der Preisberechnung ausreichend)
- Zusätzlich anfallende Zahlartgebühren

Ein Shop muss alle anfallenden Kosten den Käufern **transparent** offenlegen. Sofern versteckte Zusatzkosten anfallen, lassen sich diese als Dark Pattern bezeichnen. Es dürfen auch keine versteckten Rabattaktionen (künstlich erhöhte „Statt"-Preise) oder vorausgewählte Zusatzleisten aktiviert sein. Ein Kunde muss **aktiv kaufen** oder sich zu etwas verpflichten. Sobald ein User eine Aktion tätigt oder zu etwas verleitet wird, zu dem er vorher nicht sein wissentliches Einverständnis gegeben hat, handelt es sich um ein Dark Pattern und das sehen wir als Missbrauch an den User an. Außerdem muss durch den Kauf-Button ersichtlich sein, dass er damit eine kostenpflichtige Bestellung abgibt.

2.3.3 Zahlungsanbieter

Im Internet können keine Barzahlungen erfolgen. Daher sollten nur Zahlungsanbieter verwendet werden, die weit verbreitet sind und internationale Sicherheitsstandards wie beispielsweise den **PCI DSS** (Payment Card Industry Data Security Standard) erfüllen.

Zu solchen gehören folgende Anbieter:

- PayPal
- Klarna
- Apple Pay / Google Pay
- Amazon Pay

- Giropay / paydirekt
- Adyen
- Sofortüberweisung
- Kreditkarten über Visa / Mastercard oder American Express

Wir prüfen die angebotenen Zahlungsdienstleister auf Seriosität und Sicherheit. Anbieter sollten grundsätzlich einen **Käuferschutz** (z. B. eine Rückerstattung bei Nicht-Erhalt der Ware), ein **Rückbuchungsrecht** (Chargeback) haben und **transparent** in AGB und Datenschutzbedingungen sein.

2.3.4 Transparenz über Drittanbieter

Online Shops müssen offenlegen, ob und wann Drittanbieter agieren. Dazu gehören **Zahlungs- und Versanddienstleister**, aber auch solche für die Kommunikation, Datenverarbeitung und Marketing. Nutzer müssen klar erkennen, über welchen Anbieter Zahlungen abgewickelt werden und welche Versandpartner genutzt werden. Verarbeiten externe Tools persönliche Daten, muss dies eindeutig gekennzeichnet sein. Nur dadurch können Kunden fundierte Entscheidungen treffen und Vertrauen in den Shop gewinnen. Sie müssen wissen, wer ihre Daten verarbeitet und mit wem sie Verträge eingehen. Im Sinne des Verbraucherschutzes und der DSGVO sind diese Informationen verpflichtend in einem Online Shop anzugeben.

2.3.5 Angaben der Lieferzeiten

User müssen darüber informiert werden, wie lange es dauert bis ihre Ware ankommt bzw. welche Lieferzeiten es in welcher Region / welchen Ländern vorherrschen. Lieferbeschränkungen müssen spätestens zu Beginn des Bestellvorgangs ausgewiesen sein. Treten unerwartete Lieferschwierigkeiten auf, muss der Kunde (meist per Mail) informiert werden.

2.3.6 Bestellprozess und -bestätigung

Der Bestellvorgang sollte klar und verständlich sein. Hierzu gehören eindeutige Formulierungen bzw. **Schritte zum Kauf** der Ware. Die Schritte Warenkorb, Adresseingabe, Zahlungsart und, falls vorhanden, Versanddienstleister wählen bis hin zur zahlungspflichtigen Bestellung, müssen für den Käufer nachvollziehbar sein. **Eingabefehler** oder unausgefüllte Pflichtfelder müssen kenntlich gemacht werden, damit sie vor Bestellabschluss korrigiert werden können.

Der Kunde muss wissen, ob das Unternehmen den Vertragstext speichert und ob er vom Kunden in dessen Konto eingesehen werden kann.

Weiterhin muss dem Kunden **vor Vertragsabschluss** eine **Übersicht** mit allen wesentlichen Eigenschaften der bestellten Ware erhalten.
Hierzu gehören:

- Produktdetails
- Gesamtpreis mit evtl. Vertragslaufzeit
- Versandkosten & zusätzlich angefallene Kosten
- Kündigungsbedingungen

Der Button für die endgültige Bestellung muss unmissverständlich darauf hindeuten, dass der Kunde nach Klick eine **zahlungspflichtige Bestellung** aufnimmt.
Auf der Bestellübersicht müssen rechtliche Seiten wie **AGB und Widerrufsbelehrung** zugänglich gemacht werden. Sollten Fragen auftreten, darf der Shop-Support nicht mehr als beim normalen Telefontarif verlangen.

Nach Absenden der Bestellung, muss der Kunde unverzüglich eine Bestellbestätigung mit AGB (und Widerrufsbelehrung – spätestens bei der Versandbestätigung) per Mail erhalten, in der die **wichtigsten Informationen** zusammengefasst sind. Das bedeutet, dass zumindest der Gesamtpreis, alle bestellten Produkte mit ihrem Preis, anfallende Versandkosten und Zusatzkosten enthalten sind. Der Online-Anbieter muss außerdem klar als Absender erkennbar sein.

2.4 DSGVO Konformität

Ein Online-Unternehmen darf nicht wahllos Daten von Usern sammeln. Diejenigen, die eingeholt und auch unter Umständen gespeichert werden, müssen angegeben werden. Der Schutz der Daten vor fremden Datenklau oder -einsicht wurde bereits in Punkt 2.2 Technische Sicherheiten abgehandelt. In diesem Punkt handelt es sich um die korrekte Datenerhebung und -speicherung. Außerdem prüfen wir die Einbindung der Schriften, da diese DSGVO-konform eingebunden sein müssen. Werden Schriften extern eingebunden, so wird beim Seitenaufruf automatisch die IP-Adresse des Nutzers weitergegeben. Da dies ohne Einwilligung kritisch sein kann, sollten **Schriften lokal** auf dem Server eingebettet werden.

Prüfung auf	Beschreibung	Relevanz
Datenschutzerklärung	Zusammen mit einem Datenschutzbeauftragten vorhanden?	●
Datensammlung	Werden nur legitime Daten eingeholt?	●
Cookie / Consent Manager	Wie lange werden welche Daten und zu welchem Zweck gespeichert? Wird deutlich welche Daten an Dritte gehen?	●
Schriftarten	DSGVO konforme Einbindung von Schriften	●

2.4.1 Datenschutzerklärung

Zunächst prüfen wir, ob eine **Datenschutzerklärung** vorhanden ist, in der alle relevanten Informationen zur Datenerhebung, -verarbeitung und -speicherung sowie die Rechte der Nutzer aufgeführt sind. In der Datenschutzerklärung eines deutschen, österreichischen oder schweizerischen Shops sollte der **Datenschutzbeauftragte** namentlich und mit Kontaktdaten genannt werden, sofern folgende Voraussetzungen erfüllt werden:

- Mehr als 20 Personen im Unternehmen, die ständig mit Kundendaten arbeiten*
- Verarbeitung sensibler Daten (z. B. medizinisch, religiös oder politisch)
- Geschäftsmodell bedarf umfangreicher Datenverarbeitung (z. B. Tracking-

Dienstleister)

- Großräumige Überwachung von Personen (z. B. Geodaten, Profiling, Tracking)

**Kleine Shops mit wenigen Mitarbeitern, die sensible Daten verarbeiten, benötigen dennoch einen Datenschutzbeauftragten!*

Unternehmen mit **Sitz außerhalb der EU**, die ihre Dienste in der EU anbieten, müssen zusätzlich einen **EU-Vertreter** benennen, der als Ansprechpartner für Kunden und Behörden fungiert. Er übernimmt die Aufgabe die DSGVO-Konformität zu prüfen und bei Nachfragen bereitzustellen.

2.4.2 Datensammlung

Welche Daten werden gesammelt? An verschiedenen Stellen der Nutzung des online Angebots werden Daten erhoben. Dies sind beispielsweise Daten, die aktiv vom Nutzer gegeben werden wie bei der Registrierung, bei Abschluss einer Bestellung, bei der Kontaktaufnahme über das Kontaktformular oder bei der Anmeldung zum Newsletter. Personenbezogene Daten dürfen nur eingeholt werden, wenn sie zur Erfüllung der angebotenen Leistung oder Abwicklung des Vertrags **tatsächlich benötigt** werden. Sensible Daten wie Gesundheitsdaten, religiöse Gesinnung oder politische Meinung dürfen nur in Ausnahmefällen und auf gesetzlicher Grundlage verarbeitet werden.

Der User muss in allgemein verständlicher, leichter Sprache auf die **Art, den Umfang und Zweck der Datenerhebung** informiert werden. Dies erfolgt in der Regel über die Datenschutzerklärung. Schon beim ersten Betreten der Seite muss ein Besucher über einen sogenannten Cookie-Banner (manchmal auch Consent Manager genannt) die Möglichkeit bekommen, einzelnen Diensten explizit zuzustimmen oder abzulehnen. Mehr zum Consent Manager im nächsten Punkt 2.5.3 Cookie / Consent Manager.

Es muss erkenntlich gemacht werden, welche Daten an **Dritte weitergegeben** werden. Dies können Versanddienstleister, Social Media Plattformen, externe Anbindungen sowie Analyse- und Marketing-Tools z. B. von Google sein. Zusätzlich sollte die **Dauer der Speicherung** der einzelnen Daten in einer Liste transparent gemacht werden, damit jeder Besucher nachvollziehen kann, wie lange ihre Informationen aufbewahrt werden (sofern sie ihren Browser-Cache nicht löschen).

Bei der **Anmeldung zum Newsletter** müssen Nutzer freiwillig der Verarbeitung zustimmen können. Best Practice hierfür das Double Opt-in-Verfahren, doch auch das Single Opt-in wird oft verwendet. Nicht erlaubt sind Opt-out-Verfahren, bei dem eine Zustimmung bereits vorausgewählt ist (z. B. Anmeldung zum Newsletter).

2.4.3 Cookie / Consent Manager

Beim ersten Aufruf einer Seite muss ein Cookie Consent Manager erscheinen, sofern Cookies eingesetzt werden, die über den grundlegenden Betrieb hinausgehen. Über den Banner kann ausgewählt werden, welchen Diensten der User zustimmt. **Vorausgewählt** dürfen lediglich **notwendige Cookies** sein, die für die korrekte Nutzung der Seite nötig sind. Checkboxen für Marketing/Statistik dürfen nicht vorausgewählt sein. Außerdem müssen die Optionen „Alle akzeptieren“ und „nur notwendige Cookies“ oder anders benannte Buttons („alle abwählen“), gleichwertig aus-/abwählbar sein. Wie die Cookies eingesetzt werden, muss deutlich erkennbar sein – ob beispielsweise zu **Tracking-, Marketing- oder Komfort-Gründen** und diese sollen auch je nach Kategorie aus- oder auch wieder abwählbar sein. Auch im **Nachhinein** müssen User wieder auf den Cookie Banner Zugriff erhalten, um ihre Präferenzen noch zu ändern. **Detaillierte Informationen** welche Daten in der Kategorie Funktional / Marketing / etc. gesammelt und verarbeitet werden, sollen über einen Link erreichbar sein. Auch **welcher Drittanbieter welche Daten** erhält, sind darüber zu kommunizieren. Auch muss die **Speicherdauer** der einzelnen Daten transparent sein.

2.4.4 Schriftarten

Kommen externe Schriftarten nicht vom Server, auf dem die Seite liegt, so wird die IP-Adresse und andere personenbezogene Daten des Nutzers an denjenigen Fontanbieter, von dem die Schriftart kommt, weitergegeben. Bestenfalls wird das jedoch verhindert, um kein Risiko einer Strafe einzugehen. Daher sollten Schriften bestenfalls selbst heruntergeladen und auf dem Server eingebettet werden.

2.5 Barrierefreiheit

Seit 2025 ist das **Barrierefreiheitsstärkungsgesetz** (BFSG) in der EU relevant. User müssen die Möglichkeit haben Barrierefreiheitstools auf der Website oder dem Shop nutzen zu können. Dies lässt sich meist über ein Plugin realisieren, über das sich die Nutzer verschiedener **Werkzeuge** bedienen können: Dazu gehört die Einstellung von Kontrasten, Einblendung eines Screenreaders und Unterstützung der Tastaturnavigation. Somit wird die Seite oder der Shop für alle gleichermaßen – unabhängig von Einschränkungen – zugänglich. Bilder müssen mit Alt-Tags beschriftet sein.

Prüfung auf	Beschreibung	Relevanz
Barrierefreiheit	Existieren Barrierefreiheitstools?	●

2.6 Rechtssicherheiten

Zu den Rechtssicherheiten zählen die Seiten Impressum, AGB, Datenschutzerklärung und Widerrufsbelehrung. Die Punkte Impressum und Datenschutz wurden bereits an vorheriger Stelle behandelt. Daher behandeln wir hier lediglich noch die AGB und Widerrufsbelehrung.

Prüfung auf	Beschreibung	Relevanz
AGB	Vorhandensein der AGB	● ●
Widerrufsbelehrung	Vorhandensein und Korrektheit	● ●

2.6.1 AGB

Die AGB müssen sowohl im **Footer** als auch im **Checkout** zu finden sein. Auch in der **Bestellbestätigungsmail** nach Abschluss der Bestellung sind die AGB im Anhang zu finden. Die AGB sollten für Laien verständlich geschrieben sein. Informationen zu **Lieferbedingungen**, **Zahlungsarten** oder **Widerrufsrecht** sollten vorhanden sein.

2.6.2 Widerrufsbelehrung

Auch die Widerrufsbelehrung muss an mehreren Stellen auffindbar sein: Sie ist im **Footer** und auch nach der Bestellung per **Mail** oder anderweitig **dauerhaft** dem Kunden zugänglich. Bereits vor endgültiger Bestellabgabe müssen Bedingungen, Fristen und das Verfahren zur Ausübung des Widerrufs offenkundig sein.
In der Erklärung sind folgende Fragen zu klären:

- Wann beginnt die Frist und wie lange ist sie ausführbar?
- Wer trägt die Kosten bei einer Rücksendung?
- Wann gilt das Widerrufsrecht eventuell nicht?
- Wurde ein Muster für einen Widerruf zur Verfügung gestellt?

Die Widerrufserklärung soll nicht zum Nachteil des Käufers formuliert sein.

2.7 SEO und Usability

Weiterhin prüfen wir den Online Shop und Websites auf Meta-Informationen und auf die Benutzerfreundlichkeit. Ersteres beeinflusst eher die Betreiber der jeweiligen Seite, da dies einen Vorteil in ihrem Ranking bringt, während zweiteres wieder für die Nutzer wertvoll ist, da sie mit einer guten Usability leichter durch den Shop oder die Seite navigieren und zu ihrem Ziel kommen.

Prüfung auf	Beschreibung	Relevanz
SEO	Sind die Meta-Informationen angegeben?	●
Usability	Benutzerfreundlichkeit in der Führung durch die entsprechende Seite	●

2.7.1 SEO

Diese Informationen sind für den Shop- oder Webseitenbetreiber wichtig, um das Ranking zu verbessern. Wir prüfen hier das Vorhandensein des Meta-Titels und der Meta-Description. Diese sind relevant für die Suchmaschinenoptimierung, die neben vielen weiteren Aspekten relevant für das Ranking sind. Ein Meta-Titel und eine Meta-Beschreibung sollten das Hauptkeyword der jeweiligen Landingpage tragen und sollte

nicht zu lang und nicht zu kurz sein. Außerdem prüfen wir auf die Überschriften-Struktur der Hauptseiten: Startseite | eine Kategorieseite | eine Unterkategorieseite. Jeweils eine als Stichprobe genügt. Sollten noch mehr Seiten im Footer verlinkt sein, prüfen wir hier stichprobenartig drei – sieben durch (je nach Quantität der Links).

2.7.2 Usability

Die Usability, oder auch Bedienbarkeit, ist wichtig für den User, um schnell und einfach zu navigieren und möglichst leicht zu dem jeweiligen Ziel zu kommen ohne lange überlegen zu müssen. Die Usability ist ein Qualitätsmerkmal von Websites, denn daran erkennt man, wie viel Mühe investiert wurde, um dem User einen angenehmen Umgang zu gewährleisten. Hierzu gehören eine durchdachte Gestaltung und Strukturierung der Seite, sowohl am Desktop als auch am Tablet und am Smartphone. Auch hier gehen wir drei Seitenarten (Startseite, Kategorie- und Unterkategorieseite) durch und überprüfen diese nach:

- **Effektivität**: Z. B., dass ein bestimmtes Produkt wie geplant gefunden wird
- **Effizienz**: Dass es schnell und mit geringem Aufwand gefunden wird
- **Zufriedenheit**: Überwartungen übertroffen, da entweder schneller als erwartet oder besonders intuitiv gefunden

Besonders der letzte Punkt, die Zufriedenheit, ist heutzutage relevant, da sich die beiden ersten Punkte bereits als Standard etabliert haben.

2.8 KI-Sichtbarkeit

Die Künstliche Intelligenz (KI) ist auch in den Suchmaschinen omnipräsent: Die KI-Übersicht und -Suche stellen einen wichtigen Berührungspunkt für potenzielle Käufer oder Besucher dar. Viele User verwenden auch KI-Systeme wie ChatGPT oder Gemini bevor sie klassische Suchmaschinen verwenden. Das macht es besonders wichtig auch für KI-Suchsysteme zu ranken und die Seite dementsprechend zu optimieren.

Auch für die KI-SEO ist das klassische SEO noch relevant, jedoch ist die Semantik noch wichtiger geworden. Da wir nicht alle Texte prüfen können, schauen wir auf der

technischen Seite nach der Zugänglichkeit für Crawler über die **robots.txt**, das Vorhandensein der **LLMs.txt**, da diese für die großen Sprachmodelle (**L**arge **L**anguage **M**odels) relevant sind, und nach **strukturierten Daten** – ebenfalls relevant für die maschinelle Verarbeitung. Neben diesen Faktoren prüfen wir die **Ladezeit** der Seite, da auch diese ein wichtiger Qualitätsfaktor für KI-Bots darstellen und nach **FAQ-Schemata**, da diese gerne wegen der Frage-Antwort-Struktur herangezogen werden.

Prüfung auf	Beschreibung	Relevanz
robots.txt	Sind KI-Bots in der robots.txt Datei erlaubt und werden dementsprechend nicht blockiert?	●
LLMs.txt	Das Vorhandensein hilft KI-Bots die wichtigsten Inhalte besser zu verstehen	●
Strukturierte Daten	Existent, um genauere Antworten zu liefern?	●
Ladezeit der Seite	Ist die Ladezeit geringgehalten?	●
FAQ	FAQ-Schema werden gerne von KI-Systemen herangezogen	●

In der robots.txt kontrollieren wir, ob GPT-Bots ausgeblendet werden. Andernfalls erscheint die Seite nicht in den Suchergebnisse der KI-Systeme bzw. in der KI-Übersicht in den Suchmaschinen. Zum Verständnis und der besseren Antwortausgabe sind LLMs.txt Dateien und auch strukturierte Daten wichtig. Letzteres und auch die Ladezeit der Seite sind neben vielen anderen Aspekten auch relevant für die klassischen Suchmaschinen. Denn künstliche Intelligenzen ziehen auch SEO-relevante Seiten heran – daher ist die KI-Optimierung ein Zusatz und kein Ersatz zur SEO. Für den letzten Punkt prüfen wir das Vorkommen von FAQs. Mit diesen hat man gute Chancen, in den KI-Suchmaschinen zu erscheinen, da sie die klare Struktur von Frage – Antwort gut verstehen und demnach gerne verwenden.

3. Abschließende Worte

Mit diesem Prüfkatalog sind die zentralen Aspekte zusammengestellt, die für die Bewertung von Online Shops und Websites hinsichtlich Seriosität, Rechtssicherheit, Transparenz und Komfort abgehandelt werden müssen.

Da wir die Prüfpläne für die Öffentlichkeit zugänglich machen, hilft er einerseits den Usern, um nachzuvollziehen, wie viel Vertrauen und Sicherheiten sie auf dem Shop / der Seite erwarten können und andererseits dem Betreiber, um zu wissen, welche Verbesserungen vorzunehmen sind.

Am Ende geht es nicht nur darum, die gesetzlichen Mindestanforderungen zu erfüllen, sondern auch Vertrauen aktiv aufzubauen. Denn Vertrauen ist mit der wichtigste Baustein einer erfolgreichen online Unternehmung.

Das Gütesiegel und auch dieser Prüfkatalog können sich mit der Zeit aufgrund neuer Gesetze oder Gesetzesänderungen wandeln. Daher empfehlen wir eine **jährliche Prüfung**, die dann zu einem vergünstigten Preis von Trusted Heroes durchgeführt wird, sofern dies gewünscht ist. Die Zeit, in der der Prüfkatalog seine Gültigkeit hat, ist der Fußzeile zu entnehmen. Die **Version des Prüfkatalogs** befindet sich auch in der Fußzeile der Prüfpläne der einzelnen geprüften Shops / Websites.