Readiness von Onlineshops für KI-Agenten: Checkliste für Deutschland und die EU

Anwendungsbereich

- Die Checkliste richtet sich an Onlineshops, die Waren an Verbraucher in Deutschland verkaufen. Bei einer Tätigkeit in anderen EU-Ländern sind zusätzlich die jeweiligen nationalen Anforderungen zu prüfen.
- Technische Maßnahmen werden je nach Szenario ausgewählt: Produktsuche und -vergleich, Vorbereitung des Warenkorbs oder Kaufabschluss.
- Welche rechtlichen Anforderungen gelten, hängt von Warenkategorie, Rolle des Verkäufers, Unternehmensgröße und Ausgestaltung des Dienstes ab.
- Stand: 16. November 2026.

1. Strukturierter und aktueller Katalog

☐ Für jedes Produkt und jede kaufbare Variante werden stabile Kennungen verwendet; GTIN und MPN werden übermittelt, sofern sie vergeben sind und vom gewählten Kanal verlangt werden.

☐ Name, Beschreibung, Merkmale, Variante, Preis, Währung, Verfügbarkeit und Bilder liegen in einem Format vor, das der Datenempfänger unterstützt.

☐ Für die gewählten Kanäle sind geeignete Wege der Datenübermittlung eingerichtet: Markup mit `schema.org/Product` und `Offer`, Produktfeeds oder APIs.

☐ Die strukturierten Daten stimmen mit den auf der Produktseite sichtbaren Informationen überein.

☐ Für jeden Kanal sind die Aktualisierungsfrequenz des Katalogs und die zulässige Verzögerung bei Änderungen von Preisen und Verfügbarkeit festgelegt.

☐ Vor dem Kaufabschluss prüft das System das aktuelle Angebot und den Gesamtpreis erneut; Feeddaten werden nicht als alleinige Bestätigung der Kaufbedingungen verwendet.

☐ Beschreibungen enthalten überprüfbare Produktangaben; Merkmale, Einschränkungen und Lieferumfang sind eindeutig angegeben.

2. Datenzugänglichkeit und Szenariotests

☐ Für die gewählten Suchmaschinen und Agentendienste sind die Einstellungen für Crawling, Indexierung, CDN und Bot-Schutz geprüft.

☐ Nicht öffentliche Bereiche, personenbezogene Daten und Administrationsfunktionen sind durch Authentifizierung und Autorisierung geschützt; `robots.txt` dient zur Steuerung des Crawlings.

- ☐ Markup, Feeds und APIs sind mit den Validierungstools des jeweiligen Kanals geprüft; festgestellte Fehler sind behoben.
- ☐ Tests für Produktsuche, Variantenauswahl, Vergleich der Konditionen und Übergang zum Kauf wurden durchgeführt.
- ☐ In den Testergebnissen sind Dienst, Tool, Modell oder Version, Datum und geprüfte Szenarien dokumentiert.

3. Integrationen und Kaufabschluss

- ☐ Es ist festgelegt, welche Vorgänge externen Agenten erlaubt sind: Lesen des Katalogs, Anlegen eines Warenkorbs, Aufgeben einer Bestellung oder Abruf des Bestellstatus.
- ☐ Bei Nutzung von UCP (Universal Commerce Protocol) oder ACP (Agentic Commerce Protocol) sind die Version der Spezifikation, die unterstützten Vorgänge und die Anforderungen des jeweiligen Partners dokumentiert.
- ☐ Die Verfügbarkeit der Integration für den betreffenden Markt, die Anbindungsbedingungen für Händler und die unterstützten Zahlungsarten sind geprüft.
- ☐ Für bestellbezogene Vorgänge sind Authentifizierung, Berechtigungsprüfung und Zugriffsbeschränkung eingerichtet; der User-Agent dient nur als zusätzliches Merkmal des Clients.
- ☐ Folgende Fälle wurden getestet: Preisänderung, fehlende Verfügbarkeit des Artikels, nicht verfügbare Versandart, abgelehnte Zahlung und Übergabe der Steuerung an den Käufer.
- ☐ Wiederholte Anfragen und Netzwerkausfälle werden so behandelt, dass doppelte Bestellungen und Abbuchungen verhindert werden.
- ☐ Der Käufer erhält eine Bestätigung über das Ergebnis des Vorgangs; Abruf des Bestellstatus, Kontakt zum Support und Abwicklung von Retouren sind vorgesehen.

4. Angaben zu Verkäufer, Preisen und Produkten

- ☐ Die Pflichtangaben zum Verkäufer und die Kontaktdaten gemäß § 5 DDG sind veröffentlicht.
- ☐ Preise sind einschließlich der anfallenden Steuern angegeben; Angaben zu Versand und zusätzlichen Kosten sind gemäß PAngV offengelegt.
- ☐ Für die betreffenden Waren ist der Grundpreis – der Preis je festgelegte Mengeneinheit – angegeben.
- ☐ Bei der Bekanntgabe von Preisermäßigungen werden die anwendbaren Regeln des § 11 PAngV eingehalten, einschließlich der Angabe des niedrigsten Preises der vorangegangenen 30 Tage.
- ☐ Für Produkte im Anwendungsbereich der GPSR enthält das Fernabsatzangebot die in Artikel 19 GPSR vorgesehenen Informationen: Angaben zum Hersteller, gegebenenfalls zur verantwortlichen Person in der EU, zur Identifizierung des Produkts sowie Warnhinweise zur Sicherheit.

- ☐ Für die jeweilige Produktkategorie sind zusätzliche Anforderungen an Kennzeichnung, Sicherheit und Pflichtinformationen geprüft.

5. Verbraucherrechte und Bestellbestätigung

- ☐ Vor Vertragsschluss erhält der Käufer die anwendbaren Informationen nach § 312d BGB und Art. 246a EGBGB, einschließlich der Zahlungs-, Liefer- und Widerrufsbedingungen.
- ☐ Im gewählten Kaufszenario ist die Umsetzung der Anforderungen des § 312j BGB an die Informationen vor der Bestellung und an die ausdrückliche Bestätigung der Zahlungspflicht geprüft.
- ☐ Die Vertragsbestätigung wird dem Käufer gemäß § 312f BGB auf einem dauerhaften Datenträger zur Verfügung gestellt.
- ☐ Für Verträge im Anwendungsbereich des § 356a BGB ist eine elektronische Widerrufsfunktion umgesetzt: eine während der Widerrufsfrist verfügbare Funktion, eine Bestätigung über die Absendung der Erklärung und eine Mitteilung über deren Eingang.
- ☐ Die Bedingungen für freiwillige Rückgaben und gewerbliche Garantien sind getrennt von den gesetzlichen Verbraucherrechten dargestellt.
- ☐ Für Käufe über KI-Agenten sind das Verfahren zur Bestätigung von Handlungen, die Grenzen des Auftrags und der Prozess zur Bearbeitung strittiger oder fehlerhafter Bestellungen dokumentiert.

6. Bewertungen und Nachweise für Aussagen

- ☐ Veröffentlicht der Shop Verbraucherbewertungen, wird erläutert, ob und auf welche Weise deren Herkunft geprüft wird.
- ☐ Die Bezeichnung „Verifizierter Kauf“ wird nur verwendet, wenn eine entsprechende Prüfung erfolgt.
- ☐ Aussagen zu Zertifikaten, Auszeichnungen, Garantien und Testergebnissen haben eine überprüfbare Grundlage.
- ☐ Werden Kennzahlen zu Retouren oder Servicequalität veröffentlicht, sind Zeitraum, Berechnungsmethode und die berücksichtigten Bestellungen angegeben.
- ☐ Die Bedingungen für Versand, Rückgabe und Support stimmen auf der Website, in den Feeds und in den Integrationen überein.

7. Personenbezogene Daten und Sicherheit

- ☐ Zwecke, Rechtsgrundlagen und der erforderliche Umfang der Verarbeitung personenbezogener Daten sind festgelegt; der Käufer erhält die entsprechenden Informationen.
- ☐ Die Rollen des Shops und der Dienstleister sind festgelegt; bei Auftragsverarbeitung sind die erforderlichen Verträge abgeschlossen.

- ☐ Sicherheitsmaßnahmen, Speicherfristen, internationale Datenübermittlungen und die Erforderlichkeit einer Datenschutz-Folgenabschätzung (DSFA) sind geprüft.
- ☐ Dem Agenten werden nur die für den jeweiligen Vorgang erforderlichen Daten und Befugnisse bereitgestellt.
- ☐ Versuche, schädliche Anweisungen über Bewertungen, Beschreibungen, Bilder, Dokumente und andere externe Daten einzuschleusen, wurden getestet.
- ☐ Kritische Bestellparameter und zulässige Aktionen werden programmatisch geprüft; Beschränkungen der Befugnisse und Kontrollen für Vorgänge mit erhöhtem Risiko sind vorgesehen.
- ☐ Mit dem Zahlungsdienstleister sind SCA-Szenarien und anwendbare Ausnahmen geprüft; für die Karteninfrastruktur ist der Geltungsbereich von PCI DSS bestimmt.

8. Barrierefreiheit der Benutzeroberflächen und eigener KI-Assistent

- ☐ Die Anwendbarkeit des BFSG und der BFSGV einschließlich der vorgesehenen Ausnahmen ist geprüft; für erfasste Dienstleistungen ist die Barrierefreiheit der betreffenden Oberflächen und Funktionen sichergestellt.
- ☐ Tastaturbedienung, Feldbeschriftungen, Fehlermeldungen, Kontrast und der Kaufprozess mit assistiven Technologien sind geprüft.
- ☐ Informative Bilder haben passende Textalternativen; für dekorative Bilder wird ein leeres alt-Attribut verwendet, wo dies ihrem Zweck entspricht.
- ☐ Beim Einsatz eines eigenen KI-Assistenten sind die Rolle des Shops und die anwendbaren Pflichten nach dem AI Act bestimmt.
- ☐ In den anwendbaren Fällen wird die Person gemäß Artikel 50 Absatz 1 des AI Act darüber informiert, dass sie mit einer KI interagiert.

9. Inhalte, Vermarktung und Messung

- ☐ Inhalte werden aktualisiert, wenn sich Fakten, Merkmale und Bedingungen ändern; das Aktualisierungsdatum spiegelt inhaltliche Änderungen wider.
- ☐ Vergleiche, Tests und Reviews enthalten eine nachvollziehbare Methodik, Quellen und die Grenzen der Schlussfolgerungen.
- ☐ Die Sichtbarkeit der Produkte wird anhand einer festen Auswahl von Diensten, Anfragen, Sprachen und Regionen geprüft; die Ergebnisse werden unter Berücksichtigung der Variabilität der Antworten bewertet.
- ☐ Zugriffe aus KI-Diensten und bestätigte Bestellungen über Integrationen werden getrennt erfasst; die Grenzen der Attribution sind in den Berichten ausgewiesen.
- ☐ Für die Webanalyse ist die Einhaltung der DSGVO und des § 25 TDDDG in den anwendbaren Fällen geprüft.

- ☐ Bezahlte Platzierungen werden als eigener Werbekanal bewertet; dabei werden Verfügbarkeit, Bedingungen und Ergebnisse geprüft. Bei ChatGPT wird die Trennung der Werbung von der organischen Antwort berücksichtigt.

10. Abnahme und Aufrechterhaltung der Readiness

- ☐ Für jeden anwendbaren Punkt sind die verantwortliche Person, die Prüfmethode und der Nachweis des Ergebnisses festgelegt.
- ☐ Die Readiness für die Auffindbarkeit von Produkten und die Readiness für den Kaufabschluss werden getrennt bewertet.
- ☐ Für jeden angebundenen Kanal wurden die vereinbarten Haupt- und Fehlerszenarien erfolgreich durchlaufen.
- ☐ Vor dem Start sind festgestellte kritische Probleme in den Bereichen Sicherheit, Pflichtinformationen und Kaufabschluss behoben.
- ☐ Die Prüfungen werden nach wesentlichen Änderungen an Katalog, Benutzeroberflächen, Integrationen, Spezifikationen und anwendbaren Anforderungen wiederholt.

Quellen

Stand der Quellenprüfung: 16. November 2026.

Gesetze, Branchenspezifikationen, technische Dokumentation und Forschungsmaterialien sind getrennt aufgeführt.

Katalog, Suche und Inhalte

- Google Search Central – Merchant listing structured data. Markup für Product und Offer, Preise, Verfügbarkeit, Versand und Rückgabe.
- Google Search Central – AI features and your website. Zugänglichkeit von Inhalten für AI Overviews und AI Mode, technische Anforderungen und Übereinstimmung des Markups mit dem Seiteninhalt.
- Google Search Central – Creating helpful, reliable, people-first content. Verlässlichkeit, Nützlichkeit und substanzielle Aktualisierung von Inhalten.
- Google Search Central – A guide to Google Search ranking systems. Anwendung von Aktualitätssignalen in Abhängigkeit von der Suchanfrage.
- OpenAI Developers – Submit product feeds. Übermittlung des Produktkatalogs und Abgrenzung zwischen Feed, Browser-Aktionen und Kauf.
- OpenAI Developers – Products. Anforderungen an die Felder des Produktfeeds.

Protokolle und Agentenzugriff

- Universal Commerce Protocol – Specification Overview, Version 2026-04-08. Architektur von UCP, Aushandlung von Fähigkeiten, Identifizierung und Authentifizierung der Beteiligten.
- Agentic Commerce Protocol – Introduction. Zweck von ACP und Zusammenwirken der am Kauf Beteiligten.

- Agentic Commerce Protocol – Checkout. Vorgänge des Kaufabschlusses, Authentifizierung, API-Versionen und Behandlung wiederholter Anfragen.
- Agentic Commerce Protocol – offizielles Repository. Versionierte Spezifikationen, Schemas und Änderungsprotokoll.
- IETF – RFC 9309: Robots Exclusion Protocol. Regeln für robots.txt und Grenzen dieses Mechanismus.

Sicherheit von KI-Systemen

- OWASP GenAI Security Project – LLM01:2025 Prompt Injection. Direkte und indirekte Einschleusung von Anweisungen, Beschränkung von Befugnissen und Maßnahmen zur Risikominderung.
- OWASP GenAI Security Project – LLM06:2025 Excessive Agency. Risiken übermäßiger Funktionen, Berechtigungen und Autonomie eines Agenten.
- StakeBench – offizielles Repository der Studie. Szenarien und Methodik der Untersuchung von Prompt Injection bei Web-Agenten im E-Commerce; Forschungsmaterial.

Deutsches Recht

- Digitale-Dienste-Gesetz – § 5 DDG. Pflichtangaben des Anbieters digitaler Dienste.
- Preisangabenverordnung – PAngV. Gesamtpreis, Grundpreis, Angaben zu zusätzlichen Kosten und Regeln für die Bekanntgabe von Preisermäßigungen; insbesondere §§ 2–6 und 11.
- Bürgerliches Gesetzbuch – § 312d BGB. Informationspflichten bei Fernabsatzverträgen.
- Einführungsgesetz zum Bürgerlichen Gesetzbuche – Art. 246a § 1 EGBGB. Dem Verbraucher zur Verfügung zu stellende Informationen.
- Bürgerliches Gesetzbuch – § 312j BGB. Anforderungen an die Gestaltung der Verbraucherbestellung und an die Bestätigung der Zahlungspflicht.
- Bürgerliches Gesetzbuch – § 312f BGB. Bestätigung des Vertrags auf einem dauerhaften Datenträger.
- Bürgerliches Gesetzbuch – §§ 312g, 355–356a BGB. Widerrufsrecht, Ausnahmen, Fristen und elektronische Widerrufsfunktion:
    - § 312g – Widerrufsrecht
    - § 355 – Widerrufsrecht bei Verbraucherverträgen
    - § 356 – Widerrufsrecht bei außerhalb von Geschäftsräumen geschlossenen Verträgen und Fernabsatzverträgen
    - § 356a – Elektronische Widerrufsfunktion bei Fernabsatzverträgen
- Gesetz gegen den unlauteren Wettbewerb – § 5b Abs. 3 UWG. Information über die Prüfung der Herkunft von Verbraucherbewertungen.
- Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – § 25 TDDDG. Speicherung von Informationen in der Endeinrichtung des Nutzers und Zugriff darauf.
- Barrierefreiheitsstärkungsgesetz – BFSG. Anwendungsbereich der Barrierefreiheitsanforderungen, Pflichten und Ausnahmen; insbesondere §§ 1–3 und 14.
- Verordnung zum Barrierefreiheitsstärkungsgesetz – BFSGV. Barrierefreiheitsanforderungen, einschließlich zusätzlicher Anforderungen an Dienstleistungen im elektronischen Geschäftsverkehr nach § 19.

Recht der Europäischen Union

- Verordnung (EU) 2016/679 – DSGVO / GDPR. Grundsätze und Rechtsgrundlagen der Verarbeitung, Informationspflichten, Verhältnis zu Auftragsverarbeitern, Sicherheit, DSFA und internationale Übermittlungen; insbesondere Artikel 5–6, 13–14, 28, 32, 35 und 44–49.
- Verordnung (EU) 2023/988 – Verordnung über die allgemeine Produktsicherheit, GPSR. Sicherheit von Verbraucherprodukten; Artikel 19 – Informationen bei Fernabsatzangeboten.
- Verordnung (EU) 2024/1689 – AI Act. Anwendungsbereich, Rollen der Akteure und Transparenzanforderungen, einschließlich Artikel 50.
- Richtlinie (EU) 2015/2366 – PSD2. Artikel 97 – starke Kundenauthentifizierung bei Zahlungsvorgängen.
- Delegierte Verordnung (EU) 2018/389. Technische Anforderungen an die starke Kundenauthentifizierung und anwendbare Ausnahmen.

Barrierefreiheit und Zahlungsstandards

- W3C Web Accessibility Initiative – An alt Decision Tree. Wahl der Textalternative in Abhängigkeit vom Zweck des Bildes.
- PCI Security Standards Council – PCI Data Security Standard. Zweck von PCI DSS und Anwendungsbereich des Standards.
- PCI Security Standards Council – Document Library. Offizielle Bibliothek mit dem Standard PCI DSS und begleitenden Dokumenten.

Werbung in KI-Diensten

- OpenAI Help Center – Ads in ChatGPT. Trennung von Werbeplatzierungen und ChatGPT-Antworten, Anzeigebedingungen und Einschränkungen der Verfügbarkeit.

Haftungsausschluss

Diese Checkliste dient ausschließlich der allgemeinen Information. Sie stellt keine Rechtsberatung und keine Rechtsdienstleistung im Sinne des Rechtsdienstleistungsgesetzes (RDG) dar und ersetzt nicht die individuelle Prüfung des Einzelfalls durch eine Rechtsanwältin oder einen Rechtsanwalt.

Die Checkliste wurde auf Grundlage öffentlich zugänglicher Quellen erstellt; maßgeblich ist der Stand vom 16. November 2026. Gesetze, Rechtsprechung, technische Spezifikationen und Plattformrichtlinien können sich jederzeit ändern. Trotz sorgfältiger Erstellung wird keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte übernommen.

Eine Haftung für Schäden, die sich aus der Verwendung der Inhalte ergeben, ist ausgeschlossen, soweit dies gesetzlich zulässig ist. Für die Inhalte verlinkter externer Websites sind ausschließlich deren Betreiber verantwortlich.