Sec-IT

Mehr Sicherheit.
Mehr Wert.

Anforderungskatalog zur Bewertung und Zertifizierung von Online-Vertragsabschlüssen

Version 5.1
Stand: 2019-09-19

Hinweis: Dieser Anforderungskatalog wird auf verschiedene Arten von Online-Vertragsabschlüssen angewendet (z.B. Kauf von Waren/Dienstleistungen, Buchung von Reiseleistungen, Abschluss von Versicherungsverträgen). Der Schwerpunkt der Zertifizierung liegt auf einer Betrachtung des Vertriebskanals Internet. Eine Bewertung der (Versicherungs-)Produkte ist nicht Gegenstand der Begutachtung

Inhaltsverzeichnis

1 Organisatorische Anforderungen 2
2 Datensicherheit 2
3 Datenschutz 3
4 Online-Inhalte und Prozesse 4
4.1 Sortiment und Inhalte 4
4.2 Allgemeine Angaben 4
4.3 Leistungsdetails, Kosten und weitere Kundeninformationen 4
4.4 Recherche, Auswahl und Bestellung / Buchung / Antragsstellung 5
4.5 Bezahlvorgang 6
4.6 Lieferung / Zustellung 6
4.7 Kundenservice 6
4.8 Widerrufsrecht (sofern zutreffend) 6
4.9 Externe Angebote 7
Anhang: Disclaimer 8

© TÜV SÜD Sec-IT GmbH

Sec-IT

1 Organisatorische Anforderungen

1.1 Zur Erfüllung aller Anforderungen aus diesem Katalog und relevanter gesetzlicher Bestimmungen sind Verantwortlichkeiten und Befugnisse vollständig und eindeutig festgelegt. Es existiert eine angemessene Stellvertreterregelung.

1.2 Es sind Verfahren wirksam, die geeignet sind, die Anforderungen umzusetzen.

1.3 Die Organisation ermittelt und bewertet regelmäßig Kundenanforderungen und die Zufriedenheit der Kunden. Das Ergebnis der Bewertung von Kundenzufriedenheit wird zur ständigen Verbesserung verwendet.

2 Datensicherheit

2.1 Um die Inhalte des Online-Angebots und die personenbezogenen Daten von Nutzern und Kunden angemessen zu schützen, existiert ein geeignetes Sicherheitskonzept. Der Anbieter setzt sich mit möglichen Bedrohungen und den daraus resultierenden Risiken auseinander. Es werden angemessene Sicherheitsmaßnahmen festgelegt.

2.2 Die im Sicherheitskonzept enthaltenen Sicherheitsmaßnahmen wirken allen relevanten Bedrohungen in angemessener Weise entgegen. Dazu werden in angemessenem Umfang auch die folgenden Maßnahmen ergriffen:

- Systeme und Applikationen sind in fachgerechter Weise installiert und werden auf einem aktuellen Sicherheitsstand gehalten.
- Es haben nur angemessen authentifizierte Personen Zugriff auf personenbezogene Daten.
- Relevante Daten werden regelmäßig gesichert.
- Zum Schutz der Privatsphäre sowie zum Schutz von Zahlungsinformationen oder anderen sensiblen Daten wird eine Verschlüsselungstechnologie nach den anerkannten Regeln der Technik eingesetzt.

2.3 Es ist ein schlüssiges Konzept für den Umgang mit Notfällen vorhanden. In diesem Konzept sind verantwortliche Personen bzw. Rollen benannt und deren Befugnisse geregelt.

Sec-IT

3 Datenschutz

3.1 Die Zuständigkeit für Datenschutzbelange ist organisatorisch festgelegt. Entsprechend geltender gesetzlicher Regelungen ist ggf. ein Datenschutzbeauftragter benannt.

3.2 Es existiert eine Übersicht über alle relevanten Verarbeitungen personenbezogener Daten.

3.3 Mitarbeiter, die mit personenbezogenen Daten in Berührung kommen, wurden hinsichtlich relevanter datenschutzrechtlicher Bestimmungen geschult.

3.4 Werden personenbezogene Daten an Dritte übermittelt oder für Dritte zur Einsicht oder zum Abruf bereitgehalten, so ist durch Vereinbarungen sicherzustellen, dass der Dritte angemessene Maßnahmen zum Schutz der Daten getroffen hat. Gleiches gilt, wenn personenbezogene Daten im Auftrag des Anbieters verarbeitet werden oder der Zugriff darauf nicht ausgeschlossen werden kann.

3.5 Ohne Einwilligung des Nutzers dürfen personenbezogene Daten nur dann verarbeitet werden, soweit dies für die Begründung, Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich ist oder gesetzlich erlaubt ist (z.B. durch berechtigte Interessen des Verantwortlichen im Rahmen einer entsprechenden Interessenabwägung legitimiert werden kann).

3.6 Elektronische Einwilligungserklärungen erfolgen durch eine eindeutige, informierte, freiwillige und bewusste Handlung des Nutzers (z.B. durch selbstständiges Aktivieren einer entsprechend beschrifteten Checkbox).

3.7 Angebote, die sich an Minderjährige richten, werden nicht dazu benutzt, ohne Wissen und Einwilligung der Erziehungsberechtigten personenbezogene Daten der kindlichen Nutzer oder von Personen aus dem häuslichen Umfeld zu erfassen, auszuwerten oder an Dritte weiterzugeben.

3.8 Der Nutzer wird über Art, Umfang und Zweck der Verarbeitung von personenbezogenen Daten unterrichtet, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Diese Unterrichtung muss stets abrufbar sein. Insbesondere ist der für die Datenverarbeitung Verantwortliche klar erkennbar und eine Kontaktmöglichkeit für Anfragen zum Datenschutz vorhanden.

3.9 Soll der Nutzer zum Zweck der Beratung, Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung des Informationsangebotes angesprochen werden, ist dieser vorab über den jeweiligen Zweck und sein jederzeitiges Widerspruchsrecht zu informieren. Diese Information kann jederzeit abgerufen werden.

3.10 Eine werbliche Ansprache von Kunden bzw. Interessenten mittels elektronischer Kommunikationsmittel (z.B. Newsletter per E-Mail) ist nur zulässig, soweit diese eingewilligt haben. Ausnahmen hiervon sind ggf. unter Berücksichtigung der wettbewerbsrechtlichen Vorgaben im Hinblick auf unzumutbare Belästigung oder anderer gesetzlicher Regelungen zulässig.

3.11 Mit jeder werblichen Ansprache erhält der Betroffene die Möglichkeit, von seinem Widerspruch unmittelbar Gebrauch zu machen (z.B. über eine Internetadresse).

3.12 Es sind Vorgehensweisen festgelegt, die dazu geeignet sind, eine korrekte Handhabung der Rechte Betroffener zu gewährleisten.

Sec-IT

4 Online-Inhalte und Prozesse

4.1 Sortiment und Inhalte

a) Es werden keine Angebote und Inhalte präsentiert, die außerhalb der rechtlichen Bestimmungen liegen. Insbesondere sind Jugendschutzbestimmungen einzuhalten.

b) Ein Online-Shop, der mit Lebensmitteln handelt, kann TÜV SÜD seine Registrierung als Lebensmittelunternehmer nachweisen.

4.2 Allgemeine Angaben

a) Dem Nutzer werden folgende allgemeine Informationen auf der Website zur Verfügung gestellt: Voller Name und Identität des Online-Anbieters sowie Anschrift, E-Mail-Adresse und Telefonnummer (keine Mehrwertnummer). Diese Angaben sind einfach auffindbar und an gut sichtbarer Stelle unmittelbar erreichbar.

b) Falls Lieferbeschränkungen bestehen, wird hierauf spätestens bei Beginn des Bestellvorgangs hingewiesen.

c) Allgemeine Vertragsbedingungen (AGB) – sofern vorhanden – sind leicht erreichbar.

4.3 Leistungsdetails, Kosten und weitere Kundeninformationen

Um Nutzern ein umfassendes Bild der Leistungen und den damit verbundenen Kosten zu vermitteln, werden die folgenden Informationen zur Verfügung gestellt:

a) Informationen vor Einleitung des Bestell- / Buchungs- bzw. Versicherungsantrags-Vorgangs:

- Wesentliche Merkmale der Ware/Dienstleitung bzw. Reise bzw. Versicherung
- Preis der Ware oder Dienstleistung bzw. Reisepreis bzw. Prämienhöhe einschließlich aller Steuern (es sei denn es geht ausschließlich um Business to Business Transaktionen) und sonstiger Preisbestandteile und ggf. zusätzlich anfallende Liefer- und Versandkosten bzw. Nebengebühren. Es ist klar ersichtlich, welche Bestandteile in den geforderten Preisen enthalten sind und in welcher Währung die Preise angegeben sind.
  Bei einer Aufgliederung der Preise ist der Endpreis besonders hervorgehoben.
  Für Online-Angebote der Reisebranche (z.B. Online-Reisebüros, -Veranstalterportale) gilt zusätzlich: Im Preis muss die zu zahlende Buchungsgebühr enthalten sein, nicht aber die Kosten für die Reise-Rücktrittsversicherung, variable Kosten für Energieverbrauch und Reinigung oder Kurtaxe. Flugpreise sind inklusive Flughafengebühr und Steuern anzugeben.
- Einzelheiten hinsichtlich der Zahlung. Dazu gehören Informationen über Zahlungswege und besondere Zahlungsbedingungen auf Seiten des Anbieters (z.B. besonderes Entgelt für ein Zahlungsverfahren).
- Einzelheiten hinsichtlich der Lieferung oder Erfüllung (insbesondere voraussichtlicher Liefertermin).

Speziell für Online-Shops (z.B. Verkauf von Waren, Dienstleistungen) und für Online-Versicherungen:

- Mindestlaufzeit des Vertrags, wenn dieser eine dauernde oder regelmäßig wiederkehrende Leistung zum Inhalt hat, sowie Kündigungsbedingungen bei Verträgen, die ein Dauerschuldverhältnis betreffen und für eine längere Zeit als ein Jahr oder für unbestimmte Zeit geschlossen werden.
- sofern zutreffend, Bestehen eines Widerrufsrechts und mögliche Ausschlüsse davon (siehe Kap. 4.8)

Speziell für Online-Angebote der Reisebranche (z.B. Online-Reisebüros, -Veranstalterportale):

- Informationen über Kündigungsmöglichkeiten und -fristen.

b) Spätestens bei Lieferung der Waren bzw. bei der Erfüllung der Dienstleistungen werden die Informationen nach Kap. 4.2 a) und 4.3 a) sowie ggf. allgemeine Vertragsbedingungen (es sei denn es geht ausschließlich um Business to Business Transaktionen) dem Kunden in Textform zur Verfügung gestellt.

4.4 Recherche, Auswahl und Bestellung / Buchung / Antragsstellung

Die Funktionen im Zusammenhang mit der Recherche, Auswahl und Bestellung von Produkten und Dienstleistungen bzw. der Buchung von Reiseangeboten bzw. einem Versicherungsantrag sind korrekt, übersichtlich und einfach handhabbar.

a) Alle relevanten Informationen (wie z.B. über Anbieter, Leistungen, Vertragsbedingungen, Datenschutz) können einfach erreicht werden. Sie sind verständlich und sinnvoll im Kontext angeboten.

b) Abfragen von Angeboten und Leistungen werden korrekt ausgeführt; die Inhalte sind logisch und konsistent.

c) Bei Eingaben durch den Nutzer kann dieser klar erkennen, welche Eingaben notwendig und welche optional sind. Dabei werden nur die für die Vertragsabwicklung erforderliche persönlichen verpflichtend erhoben.

d) Eingabefehler können erkannt und berichtigt werden.

e) Der Nutzer erkennt vorher eindeutig, wann genau er die Bestellung/Buchung vornimmt und ein Vertrag zustande kommt bzw. ein Versicherungsantrag gestellt wird. Dabei ist es für den Kunden deutlich, dass er nun bei der Bestellung/Buchung bzw. Antragsstellung angelangt ist und sein nächster Klick verbindlich ist.

f) Der Nutzer kann den Bestell-/Buchungs-/Antragsvorgang jederzeit abbrechen, ohne dass eine Bestellung/Buchung/Antragstellung getätigt wurde.

g) Der Zugang der Bestellung / Buchung bzw. des Antrags wird dem Kunden unverzüglich auf elektronischem Weg bestätigt, wobei insbesondere folgende Angaben enthalten sind: alle bestellten Produkte bzw. gebuchten/ beantragten Leistungen und deren Preise, ggf. die konkret anfallenden Versandkosten, alle sonstigen Zusatzkosten, der Gesamtpreis sowie ggf. das voraussichtliche Lieferdatum.

h1) Für Online-Shops (z.B. Kauf von Waren, Dienstleistungen, Online-Services) gilt:

- Der Nutzer erhält jederzeit einen Überblick über die ausgewählten Leistungen und deren Preise.
- Waren können einzeln vor der Bestellung wieder „zurückgelegt“ werden.
- Vor der Bestellung werden alle ausgewählten Leistungen mit Einzel- und Gesamtpreisen zusammengefasst.

h2) Für Online-Angebote der Reisebranche (z.B. Online-Reisebüros, -Veranstalterportale) gilt:

- Vor der Buchung werden alle ausgewählten Leistungen mit Angabe des Reisepreises zusammengefasst.
- Nach der Buchung erhält der Kunde – sofern zutreffend – den Nachweis einer Insolvenzversicherung mit einem Sicherungsschein gemäß § 651 k BGB.

h3) Für Online-Versicherungen gilt:

- Vor der Antragsstellung werden alle ausgewählten Leistungen mit Angabe der zu zahlenden Prämien zusammengefasst.

Sec-IT

4.5 Bezahlvorgang

Die grundlegenden Funktionen im Zusammenhang mit der Bezahlung sind korrekt, übersichtlich und einfach handhabbar.

a) Es ist einfach, sich einen Überblick über die angebotenen Bezahlverfahren zu verschaffen.

b) Einzelheiten zum Bezahlvorgang sind verständlich und sinnvoll im Kontext angeboten.

c) Dem Kunden wird mindestens eine kostenfreie, gängige Zahlungsmöglichkeit angeboten.

d) Der Kunde erhält eine Zahlungsbestätigung, die eindeutig der Bestellung/Buchung bzw. dem Versicherungsvertrag zuzuordnen ist (z.B. eindeutige Kennzeichnung auf dem Kontoauszug).

e) Werden Kreditkartentransaktionen abgewickelt, müssen die Anforderungen des Payment Card Industry Datensicherheitsstandards (PCI DSS) erfüllt sein.

4.6 Lieferung / Zustellung

a) Es existiert ein wirksames Verfahren bezüglich der zeitgerechten und vollständigen Lieferung der bestellten Produkte bzw. Zustellung von Reisedokumenten in einem angemessenen Zeitrahmen vor Beginn der Reise und innerhalb einer ggf. dem Kunden genannten Zustellfrist bzw. Antragsbearbeitung und Zustellung von Versicherungsdokumenten innerhalb der dem Kunden genannten Frist oder, wenn keine Frist genannt wurde, in einem angemessenen Zeitrahmen.

b) Bei Nichteinhalten des Liefertermins wird der Kunde umgehend informiert.

c) Für Online-Angebote der Reisebranche (z.B. Online-Reisebüros, -Veranstalterportale) gilt zusätzlich: Für den Fall, dass eine Reise abgesagt werden muss, ist der Kunde rechtzeitig über diesen Sachverhalt unter Angabe von möglichen Optionen zu informieren.

4.7 Kundenservice

Der Online-Anbieter bietet einen angemessenen Kundenservice an (z.B. Hilfestellung zur Nutzung des Online-Angebots, Detail-Informationen zu Leistungen, Abwicklung von Bestellungen/Buchungen und Reklamationen).

a) Kunden haben die Möglichkeit, mit dem Online-Anbieter Kontakt aufzunehmen. Neben einer E-Mail-Adresse sollte dem Kunden auch unter einer Telefonnummer die zügige Kontaktaufnahme zu einem angemessenen Verbindungspreis erlaubt werden.

b) Anfragen und Reklamationen von Kunden werden in einem angemessenen Zeitraum sachgerecht beantwortet.

c) Bei Ansprache des Kunden per E-Mail sind der volle Name sowie die Identität des Online-Anbieters anzugeben.

4.8 Widerrufsrecht (sofern zutreffend)

Insbesondere nicht zutreffend für Online-Angebote der Reisebranche.

a) Kunden wird ein mindestens 14-tägiges Widerrufsrecht eingeräumt soweit nicht gesetzliche Bestimmungen andere Fristen vorschreiben oder bestimmte Ausschlüsse zulassen.

b) Das Widerrufsrecht darf nicht unzulässig eingeschränkt werden.

c) Bei Widerruf werden vorab geleistete Zahlungen innerhalb von 14 Tagen zurückerstattet soweit nicht gesetzliche Bestimmungen andere Fristen vorschreiben.

d) Es ist geregelt, wer die Kosten einer Rücksendung übernimmt; ggf. wird der Kunde rechtzeitig entsprechend informiert.

Sec-IT

4.9 Externe Angebote

Online-Anbieter arbeiten ggf. mit Partnern im Frontend-Bereich zusammen in Form von eingebundenen, externen Inhalten. Folgende Anforderungen gelten für solche externen Inhalte, sofern es sich um eine Anwendung zur Recherche und Bestellung/Buchung auf Basis der Bedingungen eines unabhängigen Dritten handelt (Einbindung eines externen Services, z.B. Online-Fotoservice, Blumenversand, Reiseangebote):

- eindeutige Abgrenzung als „extern“
- Anbieterkennzeichnung und Datenschutzunterrichtung des Partners sind zugänglich.
- Datenschutz und Datensicherheit sollen bei der Auswahl der Partner ausreichend berücksichtigt werden.
- Zahlungsinformationen (wie Kreditkartennummern) müssen grundsätzlich angemessen geschützt übertragen werden (anerkannte Regeln der Technik).
- kein Gegenstand der *s@fer-shopping*-Zertifizierung

Der Auftraggeber der Zertifizierung hat eventuell erforderliche Genehmigungen für eine partielle Überprüfung solcher Partner-Inhalte zu veranlassen.

Sec-IT

Anhang: Disclaimer

Die TÜV SÜD Sec-IT GmbH (Sec-IT) hat Anforderungskataloge entwickelt, die die Voraussetzungen enthalten, unter denen das Prüfzeichen an Online-Anbieter vergeben wird.

Die Anforderungskataloge definieren innerhalb der Kernkompetenzen der Sec-IT technische und ergonomische Anforderungen sowie Anforderungen an die Organisationsstruktur bezüglich des Online-Fernabsatzes, die vor der Vergabe des Zeichens s@fer-shopping erfüllt sein müssen. Das Prüfzeichen s@fer-shopping erhalten Online-Anbieter erst nach einer sorgfältigen Prüfung gegen diese Anforderungen. Dennoch kann Sec-IT keine Garantie übernehmen, dass alle zugrundeliegenden Qualitäts- und Sicherheitsanforderungen vom Online-Anbieter immer eingehalten werden.

Die technischen und ergonomischen Anforderungen haben sich im Wesentlichen an den gesetzlichen Regelungen und Vorgaben zu orientieren. Aus diesem Grunde enthält der Anforderungskatalog auch dem Gesetzeswortlaut entsprechende Kriterien. Die Vergabe des Kennzeichens s@fer-shopping an Online-Anbieter ersetzt eine rechtliche, steuerrechtliche oder betriebswirtschaftliche Beratung nicht.

Die Prüfung des Internetangebotes auf Übereinstimmung mit dem durch die Sec-IT erstellten Anforderungskatalog beinhaltet keine rechtliche Prüfung im Sinne des Rechtsberatungsgesetzes. Insbesondere findet keine Prüfung auf Übereinstimmung mit den gesetzlichen Vorschriften statt soweit diese über die Aufstellung technischer und ergonomischer Anforderungen und das Nutzerverständnis, insbesondere das des Käufers, hinausgehen.

Die Sec-IT weist ausdrücklich darauf hin, dass mit dem Auftrag zur Überprüfung des Internet-Angebotes ein Auftrag im Sinne einer rechtlichen Beratung nicht einhergeht; individualisierte rechtliche Empfehlungen oder rechtliche Hinweise werden nicht gegeben.