Fachverband
deutscher Webseiten-Betreiber GmbH
- FdWB -

Programm-Handbuch

für die

Zertifizierung von Webseiten

mit dem Programm

„International Website Trust Standard“ (IWTS)

Stand: September 2020 Version: 1.1

Autoren: Holger Harte
Fachverband deutscher Webseiten-Betreiber (FdWB)
Rahel-Hirsch-Straße 10, 10557 Berlin
Tel.: +49 (0)30 4036 3580
Fax: +49 (0)30 4036 35899
info@fdwb.de
https://fdwb.de

Dr. habil. Rainer Friedel
Control Union Akademie – Die Nachhaltigkeitsakademie –
Dorotheastraße 30, 10318 Berlin
Tel. +49 (0)162 265 95 34
academy@controlunion.com
https://www.cu-academy.de/

Inhalt Seite

1. Der Fachverband deutscher Webseiten-Betreiber (FdWB) und die Ziele seines Zertifizierungsprogramms

Der Fachverband deutscher Webseiten-Betreiber (FdWB) unterstützt Nutzer und Endverbraucher von Webseiten, mit einem Blick auf der besuchten Webseite zu erkennen, ob die besuchte Webseite in besonderer Weise sicher und vertrauenswürdig ist. Damit wird die Nutzungsfrequenz der zertifizierten Webseiten und das Vertrauen in deren Informationen deutlich erhöht. Webseitenbetreiber schützen durch Maßnahmen ihre Webseite mit wichtigen Standards und leisten somit zusätzlich einen Beitrag der Cyber-Sicherheit durch Selbstschutz und den Schutz ihrer Besucher. Das sind entscheidende kaufmännische Vorteile sowohl für die Webseitenbetreiber als auch für die Sicherheit der Webseitenbesucher und Endverbraucher.

Fachlicher Hintergrund des Zertifizierungsprogramms sind vier qualitätsrelevante Prinzipien:

a) Der ***FdWB-Standard „*International Website Trust Standard (IWTS)“** beinhaltet eine Liste von qualitätsrelevanten Prüfkriterien, die anhand anerkannter Normen definiert wurden. Sie umfassen die Bereiche Cyber-Sicherheit, Datenschutz, Inhaberschaft und Ausweisungspflichten sowie Nutzerfreundlichkeit. Die Bereiche beinhalten die Überprüfung von vertrauensbildenden sowie sicherheitsrelevanten Maßnahmen und Angaben.
   Der Standard entlastet sowohl Webseitenbetreiber, als auch Nutzer von Webseiten, selbst über die erforderlichen Kriterien einer qualitätsorientierten Webseite im Detail Bescheid zu wissen und bei jedem Besuch zu überprüfen, weil der FdWB-Standard all dieses Wissen aggregiert. Wer dem Standard folgt ist auf der sicheren Seite. Webseitenbetreiber und Webseitennutzer können sich hierauf verlassen. Mit dem IWTS-Konformitätszeichen (Logo) gekennzeichneten Webseiten kann man vertrauen.
b) Die ***Konformitätsprüfungen*** der Kunden-Webseiten werden durch vom FdWB und von den Webseitenbetreibern unabhängigen Zertifizierungsstellen durchgeführt. Ihre Zuverlässigkeit und Neutralität werden durch Akkreditierungen, die jährlich zu absolvieren sind, gesichert.
c) Die ***Kosten für die Zertifizierung*** werden auf einem niedrigen Niveau gehalten indem neuartige, kostensparende Prüfverfahren für die Konformitätsprüfung angewendet werden. Damit ist die IWTS-Zertifizierung auch für Webseitenbetreiber erschwinglich, die nur über ein geringes Budget verfügen. Für Kunden des IWTS-Zertifizierungsprogramms ist das Konformitätszeichen kostenfrei.
d) ***Beratung*** für Webseitenbetreiber, die Unterstützung zur Herstellung zertifizierungsfähiger Webseiten benötigen, leistet der FdWB und mit ihm kooperierenden Anbietern von Webseitenservices.

Hauptziele des IWTS-Programms sind:

- Webseitenanbietern wird ermöglicht, auf dem Webseitenmarkt werblich mitzuteilen, dass ihre Webseite durch eine unparteiische dritte Seite überprüft wurde, mit dem Ergebnis, dass sie alle Anforderungen des FdWB-Standards erfüllt.
- Das IWTS-Programm soll Webseitennutzer dabei unterstützen, Webseiten hinsichtlich Sicherheit und anderen Nutzungskriterien zu unterscheiden und solchen den Vorzug zu geben, die mehr Sicherheit und Service bieten. Bei Webseitennutzern wird vertrauen geschaffen, die ein Interesse an sicheren Webseiten haben.
- Bereitstellung eines kaufmännischen Vorteils für zertifizierte Webseiten.

Dieses Handbuch fixiert die Kriterien, die durch Webseitenbetreiber einzuhalten sind und sämtliche Teilprozesse des Zertifizierungsverfahrens. Es ist für alle Beteiligten am Zertifizierungsprozess, insbes. Zertifikatsinhaber und Zertifizierungsstellen verbindlich.

Der FdWB wird die Aktualität der Kriterien und die im Arbeitsprozess gewonnenen Erfahrungen zum Zertifizierungsprozess sorgfältig überwachen, dies in regelmäßigen Abständen mit dem Beirat auswerten sowie bei erkanntem Bedarf umgehend Programmanpassungen durchführen. Diese werden schriftlich an die einbezogenen Zertifizierungsstellen und Zertifikatsnutzer übermittelt. Bei sehr

wesentlichen Programmanpassungen oder zur Integrierung einer größeren Anzahl kleinerer Programmanpassungen wird eine fortgeführte Version des IWTS-Programms erstellt.

Dieses Handbuch wurde mit größter Sorgfalt erarbeitet. Wenn Leser Lücken finden, bittet der FdWB ihm diese Beobachtungen mitzuteilen.
Es wird keine Verantwortung für Fehler oder Irrtümer übernommen. Hieraus können an den FdWB keine Gewährleistungsansprüche abgeleitet werden.

2. Zweck dieses Handbuchs

Das Programmhandbuch für das IWTS-Zertifizierungsprogramm dient der Beschreibung der Ziele und der Funktion der Programmelemente, um für alle Beteiligten Transparenz zu schaffen für die gleichartige Anwendung durch alle Beteiligten.

3. Begriffsdefinitionen

Anerkannte Zertifizierungsstelle ist eine Zertifizierungsstelle, die von einer nationalen Akkreditierungsstelle akkreditiert ist und vom IWTS-Programmeigner nach dem, in diesem Programm-Handbuch beschriebenen Anerkennungsverfahren (Kapitel 6.3.4) anerkannt ist.

Anerkannter Auditor ist eine Person, die in diesem Programmhandbuch definierten fachlichen und personellen Anforderungen erfüllt und auf der Basis dieser Konformität von der Zertifizierungsstelle für seine Tätigkeit im IWTS-Programm anerkannt ist. Es dürfen nur anerkannte Auditoren für diese Tätigkeit eingesetzt werden (Kapitel 6.2.1, Punkte d) und e)).

Audit Prüfung der Konformität einer Webseite mit dem FdWB -Standard durch einen anerkannten Auditor von einer anerkannten Zertifizierungsstelle. Audits können als Vor-Ort-Audits und als Desk-Audits erfolgen. Sie lehnen sich an die Vorschriften der ISO 19001 an.

Beirat ist ein Gremium welches das reale Funktionieren des IWTS-Programms unterstützt. Der Beirat berät die Geschäftsführung des FdWB. Er arbeitet auch als Schlichtungskomitee bei Widersprüchen von Zertifizierungsstellen oder von Kunden, wenn der Sachverhalt über die Verantwortlichkeit der Zertifizierungsstelle hinausgeht. Er sollte repräsentativ die „interessierten Kreise“ vertreten und nicht mehr als 5 Personen umfassen.

Benchmarking ist ein systematischer und dokumentierter Leistungsvergleich verschiedener Zertifizierungsprogramme; meist mit dem Ziel eine Kooperation der Programme zu prüfen bzw. zu realisieren. Damit werden üblicherweise wirtschaftliche Vorteile für Programmeigner, Zertifizierungsstellen und Zertifikatsnutzer angestrebt (Kapitel 6.3.8).

Beratung ist im vorliegenden Zusammenhang die Tätigkeit, einem Webseitenbetreiber Unterstützung zu geben, Webseiten zu planen, zu entwickeln, zu betreiben oder zu vermarkten. Zertifizierungsstellen ist diese Tätigkeit nicht erlaubt, um Interessenkonflikte bei ihrer Zertifizierungsentscheidung zu vermeiden.
Für den FdWB gilt das Beratungsverbot nicht.

Beteiligte des IWTS-Programms sind: der Programmeigner Fachverband deutscher Webseiten-Betreiber GmbH (FdWB) und seine Organe, alle anerkannten Zertifizierungsstellen und alle Zertifikatsinhaber (=Webseitenbetreiber).

FdWB-Standard ist Beschreibung aller Webseiteneigenschaften (= Anforderungen an die Webseite) der Webseitenbetreiber, die für die Erreichung der Ziele des FdWB-Zertifizierungsprogramms erforderlich sind (Kapitel 5.4).

Interessent ist ein Webseitenbetreiber, der sich für die Zertifizierung gegen den FdWB-Standard interessiert, jedoch noch keinen Antrag an eine Zertifizierungsstelle abgegeben hat.

Interessierte Kreise (Stakeholder) sind natürliche oder juristische Personen sowie weitere Gruppen, die sich am IWTS-Programm beteiligt oder von ihm betroffen fühlen (z. B. Webseitenbetreiber, Webseitennutzer, Zertifizierungsstellen, Kunden, Behörden u.a.).

Konformität mit allen Anforderungen, die im FdWB-Standard beschrieben sind, ist eine Voraussetzung für die Erteilung eines Zertifikats. Dabei ist sicherzustellen, dass die Produktanforderungen und die Zertifizierungsanforderungen gleichermaßen vollständig erfüllt sind.

Nutzer von Webseiten sind juristische oder natürliche Personen, besonders Endverbraucher, die Webseiten benutzen. Sie sind üblicherweise keine Experten zur Funktionalität und Sicherheit von Webseiten. Aber sie sind daran interessiert zu wissen, ob die besuchte Webseite sicher und vertrauensvoll ist. Das IWTS-Logo gibt mit einem Blick die gewünschte positive Auskunft und schafft so für den Webseitenbetreiber kaufmännisch nutzbringendes Vertrauen.

Produktanforderungen sind die Kriterien für alle Eigenschaften der Webseite, die im FdWB-Standard definiert sind (Kapitel 5.4). Die Spezifizierung der Kriterien erfolgt (in der Regel) durch Normen Dritter. Die Einhaltung aller Kriterien ist im Zertifizierungsprozess während des Audits komplett zu überprüfen.

Programmanpassung ist eine Maßnahme des Programmeigners, punktuellen Veränderungsbedarf im Programm zu identifizieren und zu realisieren[1] sowie an die Zertifizierungsstellen und Zertifikatsnutzer zu übermitteln. Hierfür wird das Formblatt (Anlage 1) genutzt. Ausgangspunkt für Programmanpassungen können sein: normative oder rechtliche Veränderungen an den Kriterien die im Kapitel 5.4 dieses Handbuchs beschriebenen sind. Auch Erkenntnisse zur Verbesserung von im Programmhandbuch festgelegten Prozessen können zur Programmanpassung führen.
Der Bedarf für Programmanpassungen ist vom Programmeigner zu beobachten, zu identifizieren und zu formulieren. Beabsichtigte Programmanpassungen sind dem Beirat zur Beschlussfassung vorzulegen.
Entsteht ein Bedarf für generelle Veränderungen des Programms, z.B. weil inzwischen eine größere Anzahl von Programmanpassungen erfolgten, wird vom Programmeigner eine neue Version des Programms erstellt (siehe Kapitel 6.3.5 dieses Handbuchs). Der Programmeigner darf hierzu externe Experten heranziehen. Die neue Version ist dem Beirat zur Beschlussfassung vorzulegen.

Programmeigner (Programmträger) ist eine Person oder Organisation, die für die Entwicklung und Aufrechterhaltung eines bestimmten Zertifizierungsprogramms verantwortlich ist. (ISO 17067). Programmeigner des IWTS-Programms ist der FdWB.

Prüfzeichen (Konformitätszeichen, Zertifizierungszeichen, Logo) Das IWTS-Prüfzeichen ist eine eingetragene Wort-Bild-Marke und bildet das Konformitätszeichen des IWTS-Programms. Es informiert den Nutzer einer Webseite mit einem Blick, dass diese Webseite mittels des IWTS-Programms gegen den FdWB-Standard geprüft wurde und damit über besondere Sicherheitseigenschaften verfügt. Das Zeichen ist Eigentum des Programmeigners. Es kann von allen Beteiligten am IWTS-Programm kostenlos genutzt werden, um die Webseite selbst und Dokumente, die mit dem IWTS-Programm in Verbindung stehen, als Blickfang zu markieren (Details im Kapitel 6.1.5).

Qualitätsebene Das IWTS-Programm kann verschiedene Varianten haben, global oder nach Regionen und Ländern (International, Deutsch-DE, USA-USA, China-CHN, Österreich-AUT, Schweiz-CHE u.a.). Details sind durch Fortschreibung des Programms schriftlich darzulegen.

Das *Risiko* einer Webseite wird in diesem Zertifizierungsprogramm definiert in Abhängigkeit von der Einhaltung von gesetzlichen Bestimmungen in den Bereichen Cyber-Sicherheit, DSGVO, Ausweisungspflichten laut des geltenden Telemediengesetztes und EU-Verordnungen sowie zusätzlich im IWTS-Standard definierter, weitgehender Schutzmaßnahmen.
Die Prüfpunkte des IWTS-Standards definieren den Zustand.

Webseitenbetreiber sind gewerblich, freiberuflich Tätige oder juristische Personen (keine natürlichen Personen im Sinne eines Endverbrauchers - dies sind Webseiteninhaber), die mit Hilfe einer Webseite Informationen an bestimmte Zielgruppen geben. Sie verfügen i.d.R. über kein Expertenwissen über die Sicherheit und technische Qualität einer Webseite und müssen dies von Dienstleistern erledigen lassen, ohne selbst die Qualität der Dienstleistung beurteilen zu

[1] Der Programmeigner hierzu externe Experten heranziehen.

können. Die Anwendung eines Qualitäts- und Sicherheitsstandards, dessen Konformität mit dem Standard zertifiziert ist, gibt dem Webseitenbetreiber Vertrauen in seine eigene Webseite und kaufmännische Vorteile, wenn auch die Nutzer seiner Webseite mit einem Blick auf das IWTS-Logo Vertrauen in die Webseite bekommen.

Kunde ist gemäß ISO 17065 die Organisation oder Person, die gegenüber einer Zertifizierungsstelle verantwortlich dafür ist, sicherzustellen, dass die Zertifizierungsanforderungen, inkl. der Produktanforderungen, erfüllt sind. Im Rahmen dieses Zertifizierungsprogramms ist der Kunde eine gewerblich, freiberuflich Tätige oder juristische Person (keine natürliche Person im Sinne eines Endverbrauchers), die verantwortlich ist für die Erfüllung der rechtlichen Anforderungen für die Sicherheit und Qualität der Webseite und als Zeichnungsberechtigter den Zertifizierungsvertrag mit der Zertifizierungsstelle signiert.
Andere Definitionen in bestimmten Rechtsvorschriften, z.B. HGB, Bürgerliches Gesetzbuch (§ 312c), Telemediengesetz (§ 5), DSGVO oder weitere, finden in diesem eng definierten Zusammenhang keine Anwendung, wenn die Regelung nicht widersprüchlich zu den gesetzlichen Regelungen ist.
Alle zertifizierten Webseitenbetreiber werden vom Programmeigner im Internet veröffentlicht (Details im Kapitel 6.3.7 dieses Handbuchs).

Zertifikat ist das Dokument, welches auf der Grundlage der Prüfung einer Webseite mit einem definierten Verfahren durch eine akkreditierte und vom FdWB zugelassene Zertifizierungsstelle bestätigt, dass diese Webseite sämtliche Kriterien des FdWB-Standards, der Bestandteil dieses Programm-Handbuchs ist, vollständig erfüllt. Das Zertifikat ist Eigentum der ausgebenden zertifizierungsstelle. Letzteres ist die Grundlage dafür, dass die Zertifizierungsstelle jederzeit dann wieder entziehen kann, wenn der Zertifikatsnutzer nicht in angemessener Zeit für die Konformität seiner Webseite mit dem FdWB-Standard sorgt.

Zertifikatsnutzer sind gewerblich-, freiberuflich Tätige oder juristische Personen (keine natürlichen Personen im Sinne eines Endverbrauchers), die auf der Grundlage eines gültigen Zertifizierungsvertrages, ein, von einer zuständigen Zertifizierungsstelle ausgestelltes Zertifikat für seine Zwecke nutzt.

Zertifizierungsanforderungen sind die gemeinsame Menge der Produktanforderungen plus der Anforderungen, die das Zertifizierungsverfahren an den Kunden stellt. Die Anforderungen an das Zertifizierungsverfahren sind wiederum die gemeinsamen Anforderungen, die das Zertifizierungsprogramm plus die Zertifizierungsstelle an den Kunden stellen. Für die erfolgreiche Zertifizierungsentscheidung sind alle Zertifizierungsanforderungen vollständig zu prüfen und zu erfüllen.

Zertifizierungsprogramm ist ein i.d.R schriftlich dargelegtes System, das die Anforderungen (= Kriterien), Regeln und Verfahren beschreibt, um bestimmte Produkte, Prozesse und Dienstleistungen zu zertifizieren. Programmeigner sollten bei der Entwicklung von Zertifizierungsprogrammen zusätzlich zu den, durch die Nutzer (Kunden) zu erfüllenden Anforderungen auch die formalen Anforderungen der ISO 17067 erfüllen. Zertifizierungsstellen, die Produkte, Prozesse und Dienstleistungen zertifizieren, sollten nach ISO 17065 akkreditiert sein. Unternehmen, die ihre Produkte, Prozesse oder Dienstleistungen zertifizieren lassen möchten, sollten sowohl die Auswahl des für sie optimal passenden Zertifizierungsprogramms als auch die Erfüllung aller Anforderungen des Zertifizierungsprogramms vor dem ersten Audit gründlich vorbereiten.

4. Inkrafttreten

Das Programm-Handbuch für die Zertifizierung von Webseiten nach dem IWTS-Programm, Stand: September 2020, Version: 1.1 tritt mit seiner Veröffentlichung am 21.09.2020 Kraft.
Es ist verbindlich für alle Beteiligten am IWTS-Programm.

5 Das IWTS-Zertifizierungsprogramm

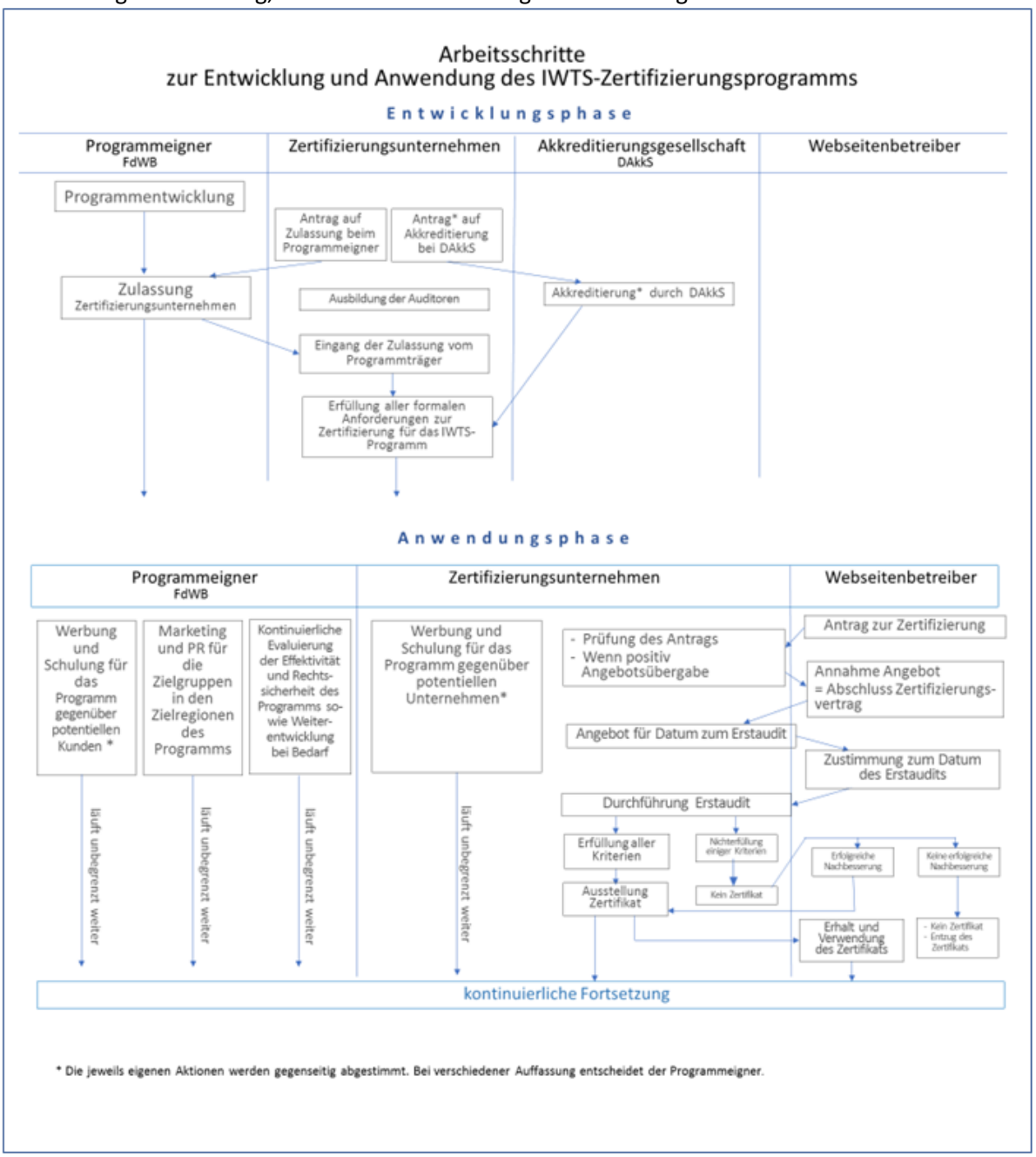
5.1 Anwendungsbereich

Dieses Handbuch beschreibt die Ziele, den Gegenstand und die Funktion des Zertifizierungsprogramms IWTS-Programm. Dieses Programm soll dafür verwendet werden, das Zusammenwirken von Programmeigner, Zertifizierungsstellen und Webseitenbetreibern so zu organisieren, dass damit für Webseitenbetreiber, die i.d.R. keine Experten für die Sicherheit und technische Funktion von Webseiten sind, das Auffinden sicherer und gut funktionierender Webseiten mit geringem Aufwand wesentlich vereinfacht wird.

Das Programm wurde unter Nutzung der ISO 17067 so angelegt, dass der Zertifizierungsprozess von neutraler dritter Seite von Zertifizierungsstellen durchgeführt wird, die ihre Arbeit auf der Grundlage des ISO 17065 durchführen.

5.2 Aufbau und Funktion des Zertifizierungsprogramms

Die Abb. 1 zeigt Entwicklung, Aufbau und Anwendung des IWTS-Programms.



5.3 Erprobungsphase

Der Programmeigner wird nach Abschluss der Programmentwicklung eine geeignete Zertifizierungsstelle gewinnen, um das Programm bis zu 2 Jahre zu erproben. Die Erprobungszeit soll dazu dienen, mit der Anwendung des Programms Erfahrungen zu sammeln und diese bei einem noch überschaubaren Umfang von Kunden auch rasch Verbesserungen des Programms vornehmen zu können.

Das detaillierte Erprobungsprogramm wird zum geeigneten Zeitpunkt gemeinsam von FdWB und der ausgewählten Zertifizierungsstelle erarbeitet und dann in der Zertifizierungspraxis praktisch angewendet.

5.4 Der FdWB-Standard für Sicherheit und Qualität

5.4.1 IWTS-Standard Variante Deutsch

Prüfbereich	**Kriterium**	**Erweiterte Hinweise für Kriterium**	**Kriterien-Nr.**	**Kriterien-ID**	**konform**	**nicht konform[1]**
Cyber-Sicherheit	URL-Test	Keine offene Weiterleitung auf andere URL nach Aufruf der Betreiber-Webseiten-URL	1	PP001	Die bei Zertifikatsantrag angegebene URL ändert sich nicht, wenn diese im Browser aufgerufen wird (keine Weiterleitung).	Die bei Zertifikatsantrag angegebene URL ändert sich nach dem Aufruf in einem Browser (Weiterleitung).
	https:// URL	Hypertext Transfer Protocol Secure (HTTPS)	2	PP002	Die im Browser aufgerufene URL zeigt von vorn beginnend zuerst diese 8 Zeichen: https://[2] Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Es werden nicht zuerst von vorne oder nicht eindeutig die 8 Zeichen https:// angezeigt.
	SSL/TLS – Secure Sockets Layer/Transport Layer Security Verschlüsselung	Funktionsprüfung SSL-/TLS-Zertifikat Kommunikationsprotokoll Transport Layer Security, starke Verschlüsselung des Kommunikationsprotokolls	3	PP003	Das SSL-/TLS-Zertifikat wird mit dem Tool "Comodo SSL Checker " (https://comodosslstore.com/ssltools/ssl-checker.php) und dem Tool "SSL Labs SSL Server Test" (https://www.ssllabs.com/ssltest) getestet und das Ergebnis enthält weder Sicherheits- noch Warnhinweise (alle Ergebnisse sind grün gekennzeichnet). Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP023 aus.	Das SSL-/TLS-Zertifikat wird mit dem Tool "Comodo SSL Checker" und dem Tool "SSL Labs SSL Server Test" getestet und das Ergebnis zeigt mindestens einen Sicherheits- oder Warnhinweis an (rot/orange gekennzeichnet). Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP023 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Beide Prüfpunkte nehmen immer direkt denselben Zustand an. Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	
	Technischer Sicherheitstest	Prüfung der Webseite auf aktuell bekannte und relevante schadhafte Systeme, Schadprogramme und Sicherheitslücken (dazu gehören u.a. Malware, Viren, offizielle Blacklists)	4	PP042	Die Prüfung der Webseite mit dem Prüf-Tool "Sucuri Site Check" (https://site-check.sucuri.net/) ergibt im Gesamtergebnis nur ein “minimales” oder höchstens “geringes" Risiko (Low) und ist somit jeweils grün. Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Die Prüfung der Webseite mit dem Prüf-Tool "Sucuri Site Check" ergibt im Gesamtergebnis ein höheres als “geringes Risiko” (Low) und ist somit orange oder rot.
Datenschutz[3]	HTTP-Cookie[4] und Cookie-Hinweis-Banner	Prüft, ob Cookies vorhanden sind und Cookie-Hinweis-Banner benötigt wird	5	PP004	Entweder a): Ein feststehendes Pop-Up-Fenster oder eine ähnliche Darstellung mit einem Cookie-Hinweis-Banner wird, spätestens nachdem die Webseite geladen wurde, angezeigt. Die Prüfung mit dem Cookie-Test-Tool "CookieMetrix" (https://www.cookie-metrix.com/) ergibt, dass Cookies der grünen Zeile oder auch weitere Cookies (orange, rote Zeile) vorhanden sind. Oder b): Ein feststehendes Pop-Up-Fenster oder eine ähnliche Darstellung mit einem Cookie-Hinweis-Banner ist nicht vorhanden und die Prüfung mit	Ein Cookie-Hinweis-Banner ist nicht vorhanden und die Prüfung mit dem Cookie-Test-Tool „CookieMetrix“ ergibt, dass außer technischer Cookies (grüne Zeile) weitere Cookies (in oranger, roter Zeile) vorhanden sind.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					dem Cookie-Test-Tool „Cookie-Metrix“ ergibt, dass nur Cookies der grünen Zeile (technische Cookies) zu sehen sind. Bei Ergebnis a) sind im Anschluss die Prüfpunkte PP005 bis PP007 zu prüfen. Bei Ergebnis b) sind die Prüfpunkte PP005 bis PP007 nicht relevant. Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	
	Cookie-Hinweistext vorhanden?	Options-Prüfpunkt	6	PP005	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis des Unterpunkts a) konform geprüft wurde: Notwendige Inhalte des Banner-Texts sind die Information, dass die Webseite Cookies verwendet, ein Hinweis auf das Widerspruchsrecht und auf den Datenschutz, mit einer Verlinkung auf die Datenschutzerklärung der Webseite. Die Datenschutzerklärung öffnet sich bei einem Klick auf den Link im gleichen oder in einem neuen Tab, einer neuen Seite oder als Banner-Element (Popup o. ä.) ("Datenschutz" und "Datenschutzerklärung" sind als Bezeichnungen zulässig).	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Wenn der Inhalt des Banner-Texts nicht die notwendigen Informationen wie Widerspruchsrecht oder Datenschutz enthält oder die Verlinkung zur Datenschutzerklärung nicht funktioniert oder nicht richtig ausgewiesen ist. Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP020 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP020 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.	
	Möglichkeit, Cookies abzulehnen	Options-Prüfpunkt	7	PP006	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis des Unterpunkts a) konform geprüft wurde: Ein Opt-out-Button[5] mit dem eindeutigen Hinweistext “keine Cookies verwenden” (oder ähnlich) oder ein eindeutiger Link auf die entsprechende Stelle der Webseite, auf der die Cookie-Nutzung per Klick abgelehnt werden kann, muss bei vorgesehener Cookie-Verwendung im Cookie-Hinweis vorhanden sein. Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP021 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Wenn kein Opt-out-Button oder kein eindeutiger Link auf die entsprechende Stelle der Webseite vorhanden ist, auf der die Cookie-Nutzung per Klick abgelehnt werden kann oder der Inhalt des Hinweistexts “keine Cookies verwenden” (verständnisgemäß oder ähnlich) weder im Cookie-Hinweis noch auf der verlinkten Seite vorhanden ist. Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP021 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.
	Möglichkeit, Cookies zu erlauben	Options-Prüfpunkt	8	PP007	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis des Unterpunkts a) konform geprüft wurde: Ein Opt-in-Button[6] oder Link muss vorhanden sein, der zur aktiven Einwilligung der Nutzung von Cookies per Klick, mit dem eindeutigen Hinweistext	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Kein Opt-in-Button oder Link ist vorhanden, der zur Nutzung von Cookies aktiv geklickt werden muss oder der nicht den eindeutigen Hinweistext "Cookies

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					“Cookies verwenden/erlauben” (oder ähnlich) geklickt werden muss. Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP022 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.	verwenden/erlauben“ (oder ähnlich) enthält. Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP022 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.
	Link zur Datenschutzerklärung	Prüfung Ausweisungspflichten	9	PP008	Es wird auf jeder beliebigen Webseite der zu prüfenden Domain im Header (oben) oder Footer (unten), gut sichtbar ein Link mit der Bezeichnung "Datenschutzerklärung" oder "Datenschutz" angezeigt, der auf die Datenschutzerklärung verlinkt. Ergebnis von einer Seite ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Es wird nicht auf jeder beliebigen Webseite der zu prüfenden Domain im Header (oben) oder Footer (unten), gut sichtbar ein Link mit der Bezeichnung "Datenschutzerklärung" oder "Datenschutz" angezeigt oder der Link verlinkt nicht auf die Datenschutzerklärung.
	Link zur Datenschutzerklärung - zusätzliche Seiten in weiteren Sprachen	Options-Prüfpunkt Prüfung Ausweisungspflichten	10	PP009	Wird die Webseite zusätzlich in englischer oder anderer Sprache angeboten, muss eine Übersetzung der Datenschutzerklärung in der jeweiligen Sprache vorhanden sein und es gelten hierfür dieselben Prüfkriterien wie für den deutschsprachigen Teil: Es wird, im Falle einer zusätzlichen englischen Sprachversion, auf jeder beliebigen Webseite der zu prüfenden Domain im Header (oben) oder Footer (unten),	Wird die Webseite zusätzlich in englischer oder anderer Sprache angeboten, muss eine Übersetzung der Datenschutzerklärung in der jeweiligen Sprache vorhanden sein und es gelten hierfür dieselben Prüfkriterien wie für den deutschsprachigen Teil: Es wird, im Falle einer zusätzlichen englischen Sprachversion, nicht auf jeder beliebigen Webseite der zu prüfenden Domain im Header (oben) oder Footer

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					gut sichtbar ein Link mit der Bezeichnung "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" oder "Data Protection Declaration" oder im Falle einer weiteren Sprache mit der Bezeichnung „Datenschutzerklärung“ oder „Datenschutz“ (bzw. ähnliche Bezeichnung) in der betreffenden Sprache angezeigt, der auf die jeweilige Sprachversion der Datenschutzerklärung verlinkt. Ergebnis von einer Seite ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	(unten), gut sichtbar ein Link mit der Bezeichnung "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" oder "Data Protection Declaration" oder im Falle einer weiteren Sprache mit der Bezeichnung „Datenschutzerklärung“ oder „Datenschutz“ (bzw. ähnliche Bezeichnung) in der betreffenden Sprache angezeigt oder der Link verlinkt nicht auf die Datenschutzerklärung in der jeweiligen Sprachversion.
	Existiert eine Datenschutzerklärung?	Prüfung Ausweisungspflichten	11	PP010	Mit einem Klick auf einen Link oder Menüpunkt “Datenschutzerklärung” wird man auf eine extra Seite weitergeleitet, die die Überschrift “Datenschutzerklärung” hat. Auf dieser Seite befindet sich ein leicht erkennbarer Text, der das Thema Datenschutz behandelt. Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Es ist nicht möglichen einen Link oder einen Menüpunkt mit der Bezeichnung “Datenschutzerklärung” zu finden oder auf der Zielseite ist keine Überschrift “Datenschutzerklärung” oder kein Textinhalt über das Thema Datenschutz vorhanden.
	Existiert eine Datenschutzerklärung? - zusätzliche Seiten	Options-Prüfpunkt Prüfung Ausweisungspflichten	12	PP011	Wird die Webseite zusätzlich in englischer oder anderer Sprache angeboten, muss eine Übersetzung der Datenschutzerklärung in der jeweiligen Sprache	Wird die Webseite zusätzlich in englischer oder anderer Sprache angeboten, muss eine Übersetzung der Datenschutzerklärung in der jeweiligen Sprache

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
	in weiteren Sprachen				vorhanden sein und es gelten hierfür dieselben Prüfkriterien wie für den deutschsprachigen Teil: Mit einem Klick auf einen Link oder Menüpunkt "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" oder "Data Protection Declaration", im Falle einer englischen Sprachversion, oder im Falle einer weiteren Sprache mit der Bezeichnung „Datenschutzerklärung“ oder „Datenschutz“ (bzw. änliche Bezeichnung) in der betreffenden Sprache, wird man auf eine extra Seite weitergeleitet, die, im Falle einer englischen Sprachversion, die Überschrift "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" oder "Data Protection Declaration oder im Falle einer weiteren Sprache die Überschrift „Datenschutzerklärung“ oder „Datenschutz“ (bzw. ähnliche Bezeichnung) in der betreffenden Sprache hat. Auf dieser Seite befindet sich ein leicht erkennbarer Text, der das Thema Datenschutz in der jeweiligen Sprache behandelt.	vorhanden sein und es gelten hierfür dieselben Prüfkriterien wie für den deutschsprachigen Teil: Es ist nicht möglichen, im Falle einer englischen Sprachversion, einen Link oder ein Menü mit der Bezeichnung "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" oder "Data Protection Declaration" oder im Falle einer weiteren Sprache, mit der Bezeichnung „Datenschutzerklärung“ oder „Datenschutz“ (bzw. ähnliche Bezeichnung) in der betreffenden Sprache zu finden oder auf der Zielseite ist, im Falle einer englischen Sprachversion, keine Überschrift "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" oder "Data Protection Declaration" bzw. im Falle einer weiteren Sprache keine Überschrift „Datenschutzerklärung“ oder „Datenschutz“ (o. ä. Bezeichnung) in der betreffenden Sprache oder kein Textinhalt über das Thema Datenschutz in der jeweiligen Sprache vorhanden.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	
	Form der Datenschutzerklärung ist übersichtlich und gegliedert	Prüfung Ausweisungspflichten	13	PP012	Die Datenschutzerklärung ist mit Überschriften, Themenblöcken, strukturierten Aufzählungszeichen und Absätzen versehen.	Die Datenschutzerklärung besteht nur aus Fließtext oder hat keinen strukturierten Charakter.
	Form der Datenschutzerklärung ist übersichtlich und gegliedert - zusätzliche Seiten in weiteren Sprachen	Options-Prüfpunkt Prüfung Ausweisungspflichten	14	PP013	Wird die Webseite zusätzlich in englischer oder anderer Sprache angeboten, muss eine Übersetzung der Datenschutzerklärung in der jeweiligen Sprache vorhanden sein und es gelten hierfür dieselben Prüfkriterien wie für den deutschsprachigen Teil: Die Datenschutzerklärung in der jeweiligen Sprache ist mit Überschriften, Themenblöcken, strukturierten Aufzählungszeichen und Absätzen versehen.	Wird die Webseite zusätzlich in englischer oder anderer Sprache angeboten, muss eine Übersetzung der Datenschutzerklärung in der jeweiligen Sprache vorhanden sein und es gelten hierfür dieselben Prüfkriterien wie für den deutschsprachigen Teil: Die Datenschutzerklärung in der jeweiligen Sprache besteht nur aus Fließtext oder hat keinen strukturierten Charakter.
	Daten des Unternehmens in der Datenschutzerklärung	Prüfung Ausweisungspflichten	15	PP014	Unter einer der Überschriften auf der Datenschutzerklärungsseite sind leicht erkennbar Unternehmensname, Adresse und Kontaktdaten[7] aufgeführt. Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Es gibt keine oder keine vollständigen Angaben des Unternehmensnamens, der Adresse und Kontaktdaten.
	Daten des Unternehmens in der	Options-Prüfpunkt	16	PP015	Wird die Webseite zusätzlich in englischer oder anderer Sprache angeboten, muss eine Übersetzung der	Wird die Webseite zusätzlich in englischer oder anderer Sprache angeboten, muss eine Übersetzung der

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
	Datenschutzerklärung - Seiten in weiteren Sprachen	Prüfung Ausweisungspflichten			Datenschutzerklärung in der jeweiligen Sprache vorhanden sein und es gelten hierfür dieselben Prüfkriterien wie für den deutschsprachigen Teil: Unter einer der Überschriften auf der Datenschutzerklärungsseite sind leicht erkennbar Unternehmensname, Adresse und Kontaktdaten aufgeführt. Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Datenschutzerklärung in der jeweiligen Sprache vorhanden sein und es gelten hierfür dieselben Prüfkriterien wie für den deutschsprachigen Teil: Es gibt keine oder keine vollständigen Angaben des Unternehmensnamens, der Adresse und Kontaktdaten.
	Hinweispflicht Datenschutzbeauftragte/r	Options-Prüfpunkt Prüfung Ausweisungspflichten	17	PP016	Dieser Prüfpunkt ist nur relevant, wenn sich durch die Antwort des Antragsstellers im Zuarbeiten-Formular herausstellt, dass ein Datenschutzbeauftragter im Unternehmen benötigt wird. Ansonsten entfällt dieser Prüfpunkt: Es muss ein/e Datenschutzbeauftragte/r mit Namen und Kontaktdaten auf der Datenschutzerklärungsseite benannt werden. Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Wenn laut Auskünften des Antragsstellers im Zuarbeiten-Formular ein/e Datenschutzbeauftragte/r im Unternehmen benannt werden muss, aber kein/e Datenschutzbeauftragte/r auf der Datenschutzerklärungsseite ausgewiesen wird.
	Web-Kontaktformular/e[8]:	Prüfung Ausweisungspflichten	18	PP017	Jedes Kontakt-/Newsletter-Formular oder sonstige Datenerfassungsformular muss sichtbar über dem Button	In mindestens einem auf der Seite angebotenem Formular fehlt der sichtbare Datenschutzhinweis der Webseite über

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
	Datenschutzhinweis				"Senden" (oder ähnliche Bezeichnung) auf die Datenschutzhinweise der Webseite, mit dem Wort "Datenschutz" oder "Datenschutzerklärung", hinweisen und mit einer "Zustimmung" verbunden sein. Für diese Prüfung müssen alle Seiten[7a] der zu zertifizierenden Webseite auf Formulare abgesucht werden. Ergebnis des vollständigen Formulars ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	dem Button "Senden" (oder ähnliche Bezeichnung), der mit dem Wort "Datenschutz" oder "Datenschutzerklärung" gekennzeichnet ist und mit einer "Zustimmung" verbunden ist. Für diese Prüfung müssen alle Seiten[7a]er zu zertifizierenden Webseite auf Formulare abgesucht werden.
	Web-Kontaktformular/e: Datenschutz Kontrollkästchen	Nicht ausgefüllte Checkbox (Kontrollkästchen)	19	PP018	Wenn das Kontaktformular als Newsletter oder für Benachrichtigungsaktionen ausgewiesen wird, welche jegliche unaufgeforderten Zusendungen an den Absender der Daten ermöglichen, muss zum Datenschutzhinweis eine nicht ausgefüllte Checkbox (Kontrollkästchen) existieren, welche vor der Versandmöglichkeit der Formulardaten aktiviert werden muss, um eine Einwilligung zum Datenschutzhinweis zu bestätigen. Für diese Prüfung müssen alle Seiten der zu zertifizierenden Webseite auf Formulare abgesucht werden.	Wenn das Kontaktformular als Newsletter oder für Benachrichtigungsaktionen ausgewiesen wird, welches jegliche unaufgeforderten Zusendungen an den Absender der Daten ermöglicht, existiert zum Datenschutzhinweis keine nicht ausgefüllte Checkbox (Kontrollkästchen), welche vor der Versandmöglichkeit der Formulardaten aktiviert werden muss, um dem Datenschutzhinweis einzuwilligen. Für diese Prüfung müssen alle Seiten der zu zertifizierenden Webseite auf Formulare abgesucht werden.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Ergebnis des vollständigen Formulars ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	
	Web-Kontaktformular/e: Personenbezogene Datenerfassung	Kein pauschales Datensammeln, keine pauschalen Pflichtfelder	20	PP019	Es werden nur notwendige Daten wie Anrede, Name, E-Mail-Adresse, Betreff und Textnachricht in einem Kontaktformular durch definierte Pflichtfelder abgefragt. Alle anderen abgefragten Daten dürfen keine Pflichtfelder sein. Handelt es sich um eine Newsletter-Anmeldung, darf nur das E-Mail-Feld ein Pflichtfeld sein. Für diese Prüfung müssen alle Seiten der zu zertifizierenden Webseite auf Formulare abgesucht werden. Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP024 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.	Es werden in einem Kontaktformular über die Daten oder Fragen wie Anrede, Name, E-Mail-Adresse, Betreff, Textnachricht bzw. bei einer Newsletter-Anmeldung über das E-Mail-Feld hinaus weitere Daten abgefragt, die als Pflichtfelder gekennzeichnet sind oder ohne deren Eingabe das Absenden des Formulars/der Anmeldung technisch verhindert wird. Für diese Prüfung müssen alle Seiten der zu zertifizierenden Webseite auf Formulare abgesucht werden. Das Ergebnis der Prüfung dieses Punktes wirkt sich direkt auf PP024 aus. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.
	Auskunftsrecht-Aufklärungspflicht (personalisierte Daten)	Prüfung Datenschutz DSGVO/TMG	21	PP020	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Notwendige Inhalte des Banner-Texts sind die Information, dass die Webseite Cookies verwendet, ein Hinweis auf das Widerspruchsrecht und auf den	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Wenn der Inhalt des Banner-Texts nicht die notwendigen Informationen wie Widerspruchsrecht oder Datenschutz enthält oder die Verlinkung zur

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Datenschutz, mit einer Verlinkung auf die Datenschutzerklärung der Webseite. Die Datenschutzerklärung öffnet sich bei einem Klick auf den Link im gleichen oder in einem neuen Tab, einer neuen Seite oder als Banner-Element (Pop-up o. ä.) ("Datenschutz" und "Datenschutzerklärung" sind als Bezeichnungen zulässig). Das Prüfvorgehen dieses Prüfpunkts entspricht PP005. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.	Datenschutzerklärung nicht funktioniert oder nicht richtig ausgewiesen ist. Das Prüfvorgehen dieses Prüfpunkts entspricht PP005. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.
	Auskunftsrecht-Ablehnung (personalisierte Daten)	Prüfung Datenschutz DSGVO/TMG	22	PP021	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Ein Opt-out-Button mit dem eindeutigen Hinweistext “keine Cookies verwenden” (oder ähnlich) oder ein eindeutiger Link auf die entsprechende Stelle der Webseite, auf der die Cookie-Nutzung per Klick abgelehnt werden kann, muss bei vorgesehener Cookie-Verwendung im Cookie-Hinweis vorhanden sein. Das Prüfvorgehen dieses Prüfpunkts entspricht PP006. Beide Prüfpunkte	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Wenn kein Opt-out-Button oder kein eindeutiger Link auf die entsprechende Stelle der Webseite vorhanden ist, auf der die Cookie-Nutzung per Klick abgelehnt werden kann oder der Inhalt des Hinweistexts “keine Cookies verwenden” (verständnisgemäß oder ähnlich) weder im Cookie-Hinweis noch auf der verlinkten Seite vorhanden ist. Das Prüfvorgehen dieses Prüfpunkts

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					nehmen immer direkt denselben Zustand an.	entspricht PP006. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.
	Einwilligung in die Datenverarbeitung von Dritten (personalisierte Daten)	Prüfung Datenschutz DSGVO/TMG	23	PP022	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Ein Opt-in-Button oder Link muss vorhanden sein, der zur aktiven Einwilligung der Nutzung von Cookies per Klick, mit dem eindeutigen Hinweistext “Cookies verwenden/erlauben” (oder ähnlich) geklickt werden muss. Das Prüfvorgehen dieses Prüfpunkts entspricht PP007. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.	Dieser Prüfpunkt ist relevant, wenn PP004 auf Basis der Unterpunkt a) konform geprüft wurde: Kein Opt-in-Button oder Link ist vorhanden, der zur Nutzung von Cookies aktiv geklickt werden muss oder der nicht den eindeutigen Hinweistext "Cookies verwenden/erlauben) (oder ähnlich) enthält. Das Prüfvorgehen dieses Prüfpunkts entspricht PP007. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.
	Sichere Datenübertragung (im Internet)	Prüfung Datenschutz DSGVO/TMG	24	PP023	Das SSL-/TLS-Zertifikat wird mit dem Tool "Comodo SSL Checker" (https://comodosslstore.com/ssltools/ssl-checker.php/) und dem Tool "SSL Labs SSL Server Test" (https://www.ssllabs.com/ssltest/) getestet und das Ergebnis enthält weder Sicherheits- noch Warnhinweise (alle Ergebnisse sind grün gekennzeichnet). Das Prüfvorgehen dieses Prüfpunkts entspricht PP003. Beide Prüfpunkte	Das SSL-/TLS-Zertifikat wird mit dem Tool "Comodo SSL Checker" und dem Tool "SSL Labs SSL Server Test" getestet und das Ergebnis zeigt mindestens einen Sicherheits- oder Wahrhinweis an (rot/orange gekennzeichnet). Das Prüfvorgehen dieses Prüfpunkts entspricht PP003. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					nehmen immer direkt denselben Zustand an.	
	Kein pauschales Datensammeln (mit Formularen)	Prüfung Datenschutz DSGVO/TMG	25	PP024	Es werden nur notwendige Daten wie Anrede, Name, E-Mail-Adresse, Betreff und Textnachricht in einem Kontaktformular durch definierte Pflichtfelder abgefragt. Alle anderen abgefragten Daten dürfen keine Pflichtfelder sein. Handelt es sich um eine Newsletter-Anmeldung, darf nur das E-Mail-Feld ein Pflichtfeld sein. Das Prüfvorgehen dieses Prüfpunkts entspricht PP019. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.	Es werden in einem Kontaktformular über die Daten oder Fragen wie Anrede, Name, E-Mail-Adresse, Betreff, Textnachricht bzw. bei einer Newsletter-Anmeldung über das E-Mail-Feld hinaus weitere Daten abgefragt, die als Pflichtfelder gekennzeichnet sind oder ohne deren Eingabe das Absenden des Formulars/der Anmeldung technisch verhindert wird. Das Prüfvorgehen dieses Prüfpunkts entspricht PP019. Beide Prüfpunkte nehmen immer direkt denselben Zustand an.
Inhaberschaft	Domain-Inhaberschaft bzw. Nutzungs-Berechtigung	Berechtigung URL-Nutzung	26	PP025	Der Auftraggeber hat im Zuarbeiten-Formular bestätigt, dass er den Key für die Domain-Inhaber-Verifikation hinterlegt hat und der Auftraggeber hat den ihm im Auftragsprotokoll ausgewiesenen Key in der Form "iwts-site-verification-[Key]" im DNS-Report seines Domain- bzw. Server-Hosters hinterlegt und die Prüfung mit dem Tool Qualidator DNS Report (https://www.qualidator.com/WQM/de/Tools/DNSReport.aspx) bestätigt, dass der Key hinterlegt wurde.	Der Auftraggeber hat im DNS-Report seines Domain- bzw. Server-Hosters keinen Key oder einen vom Auftragsprotokoll abweichenden Key hinterlegt.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Ergebnis des Prüfergebnisses mit dem DNS Report Tool ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	
	Inhaberschaft Verifizierung Registerauszug	Options-Prüfpunkt Vorab-Dokumente	27	PP026	Entweder der Antragsteller hat bei der Antragstellung angegeben, dass er Register-eintragspflichtig ist und hat vorab ein Dokument „Registerauszug“ zugesendet. Dann ist zu prüfen, ob die Unternehmens-, Inhaber-, Adress- und Registrierungsdaten des Dokuments mit den Angaben auf der zu zertifizierenden Webseite übereinstimmen. Oder der Antragsteller hat bei der Antragstellung angegeben, dass er nicht Register-eintragspflichtig ist.	Entweder der Antragsteller hat bei der Antragstellung angegeben, dass er Register-eintragspflichtig ist, hat aber vorab kein Dokument „Registerauszug“ zugesendet. Oder der Antragsteller hat bei der Antragstellung angegeben, dass er Register-eintragspflichtig ist und hat vorab ein Dokument „Registerauszug“ zugesendet. Die Unternehmens-, Inhaber-, Adress- oder Registrierungsdaten des Dokuments stimmen aber nicht mit den Angaben auf der zu zertifizierenden Webseite überein.
	Inhaberschaft Verifizierung Gewerbeanmeldung	Options-Prüfpunkt Vorab-Dokumente	28	PP027	Dieser Prüfpunkt ist nur relevant, wenn der Antragsteller in Prüfpunkt PP026 angegeben hat, dass er nicht Register-eintragspflichtig ist: Entweder der Antragsteller hat bei der Antragstellung angegeben, dass er Gewerbe-anmeldepflichtig ist und hat vorab ein Dokument „Gewerbeanmeldung“ zugesendet. Dann ist zu prüfen, ob die Unternehmens-, Inhaber-, Adress- und Registrierungsdaten des Dokuments mit den Angaben auf der zu	Dieser Prüfpunkt ist nur relevant, wenn der Antragsteller in Prüfpunkt PP026 angegeben hat, dass er nicht Register-eintragspflichtig ist: Entweder der Antragsteller hat bei der Antragstellung angegeben, dass er Gewerbe-anmeldepflichtig ist, hat aber vorab kein Dokument „Gewerbeanmeldung“ zugesendet. Oder der Antragsteller hat bei der Antragstellung angegeben, dass er Gewerbe-anmeldepflichtig ist und hat vorab

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					zertifizierenden Webseite übereinstimmen. Oder der Antragsteller hat bei der Antragstellung angegeben, dass er nicht Gewerbe-anmeldepflichtig ist.	ein Dokument „Gewerbeanmeldung“ zugesendet. Die Unternehmens-, Inhaber-, Adress- und Registrierungsdaten des Dokuments stimmen aber nicht mit den Angaben auf der zu zertifizierenden Webseite überein.
	Inhaberschaft Verifizierung Rechnungsdokument	Options-Prüfpunkt Vorab-Dokumente	29	PP028	Dieser Prüfpunkt ist nur relevant, wenn kein anderes Dokument entsprechend der Prüfpunkte PP026 oder PP027 vorliegt: Es ist zu prüfen, ob ein Dokument "Rechnungsdokument" (Verbrauchs-, Miet-, Strom- oder Internetanschlussrechnung) vorab zugesendet wurde und ob die Unternehmens-, Inhaber- oder Adressdaten mit den Angaben auf der Webseite übereinstimmen.	Dieser Prüfpunkt ist nur relevant, wenn kein anderes Dokument entsprechend der Prüfpunkte PP026 oder PP027 vorliegt: Es wurde vorab kein „Rechnungsdokument“ (Verbrauchs-, Miet-, Strom- oder Internetanschlussrechnung) vom Antragsteller zugesendet oder die Unternehmens-, Inhaber- oder Adressdaten des Dokuments stimmen aber nicht mit den Angaben auf der zu zertifizierenden Webseite überein.
	Impressum: Hinweis	Eindeutige Wahrnehmungsmöglichkeit	30	PP029	Es wird auf jeder beliebigen Webseite der zu prüfenden Domain, im Header (oben) oder Footer (unten) gut sichtbar ein Link mit der Bezeichnung "Impressum" angezeigt, der auf die Impressumsseite verlinkt. Alternativ können stattdessen auf jeder Seite gut sichtbar die vollständigen Impressumsangaben, wie in den Prüfpunkte PP031 bis PP040 verlangt, dargestellt sein.	Es wird nicht auf jeder beliebigen Webseite der zu prüfenden Domain, im Header (oben) oder Footer (unten) gut sichtbar ein Link mit der Bezeichnung "Impressum" oder die vollständigen Impressumsangaben, wie in den Prüfpunkten PP031 bis PP040 verlangt, angezeigt.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Ergebnis einer Seite ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	
	Impressum: Weiterleitungs-Link zur Impressumsseite	Link zu Impressumsseite vorhanden	31	PP030	Bei einem Klick auch den Link "Impressum" muss ein neuer Bereich oder eine neue Seite mit der Kennzeichnung Impressum und dem Impressumsinhalt sichtbar werden. Ergebnis des vollständigen Impressums ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Bei Klick auch den Link "Impressum" sind die Impressumsdaten nicht zu sehen.
	Impressum: Inhaberangaben/Unternehmensauskunft	Pflichtangaben Inhaberdaten	32	PP031	Die Angaben zu Unternehmensname, Inhaber Vor- und Nachname, Anschrift (Straße, Hausnummer, PLZ, Ort) sind vorhanden.	Es fehlt eine oder mehrere Pflichtangaben zum Unternehmen wie: Unternehmensname, Vor- und Nachname des Inhabers, Anschrift (Straße, Hausnummer, PLZ, Ort).
	Impressum: Sitz des Unternehmens		33	PP032	Der Inhaber-Geschäftssitz muss in Deutschland sein und somit eine deutsche Adresse als Impressumsangabe haben. Die deutsche Adresse muss die Geschäftsadresse sein und muss oben als erste Adresse stehen, sollte es mehrere Filialen innerhalb oder außerhalb Deutschlands geben. Zur Prüfung muss geprüft werden, dass sich die Postleitzahl der Bundesrepublik Deutschland (BRD) zuordnen lässt. Die	Die im Impressum zuoberst angegebene Adresse ist kein deutscher Standort. Die angegebene Postleitzahl existiert nicht oder befindet sich nicht in der BRD.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					eindeutige Prüfung erfolgt mit dem Tool https://www.postdirekt.de/plzserver/.	
	Impressum: Eingetragenes Unternehmen	Options-Prüfpunkt Prüfung, ob es sich um eine juristische Person handelt	34	PP033	Dieser Prüfpunkt ist nur relevant, wenn es sich beim Unternehmen der zu prüfenden Webseite um ein eingetragenes Unternehmen handelt, nicht aber bei Einzelunternehmen: Die Angabe des Antragstellers im Zertifizierungsantrag, ob es sich beim Antragsteller um eine eingetragene juristische Person handelt, wurde mit "Ja" beantwortet und ein Registerauszug, den der Antragsteller übermittelt hat, liegt als Dokumentenkopie vor.	Dieser Prüfpunkt ist nur relevant, wenn es sich beim Unternehmen der zu prüfenden Webseite um ein eingetragenes Unternehmen handelt, nicht aber bei Einzelunternehmen: Der Antragsteller hat bei Antragstellung angegeben, dass es sich beim Unternehmen um ein eingetragenes Unternehmen (als juristische Person) handelt, es liegt jedoch kein Registerauszug als Dokumentenkopie vor oder der Antragsteller hat bei Antragstellung angegeben, dass es sich beim Unternehmen um kein eingetragenes Unternehmen (als juristische Person) handelt, jedoch lässt die angegebene Unternehmensform im Impressum darauf schließen, dass es sich um ein eingetragenes Unternehmen (als juristische Person) handelt.
	Impressumangaben: Rechtsform des Unternehmens bei juristischer Person	Options-Prüfpunkt	35	PP034	Bei juristischen Personen muss die Unternehmensrechtsform[9] als Abkürzung oder ausgeschrieben hinter dem Unternehmensnamen stehen.	Beim Unternehmen handelt es sich um eine juristische Person, die Rechtsform steht aber weder abgekürzt noch ausgeschrieben hinter dem Unternehmensnamen.
	Impressumsangaben: Kontaktmöglichkeit 1		36	PP035	Es muss eine der folgenden Kontaktmöglichkeiten vorhanden sein: E-Mail-	Es ist keine der folgenden Kontaktmöglichkeiten angegeben: E-Mail-Adresse,

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Adresse, Telefonnummer, Faxnummer, Kontaktformular.	Telefonnummer, Faxnummer, Kontaktformular.
	Impressumsangaben: Kontaktmöglichkeit 2		37	PP036	Es muss eine weitere Kontaktmöglichkeit (ungleich Kontaktmöglichkeit 1) vorhanden sein: E-Mail-Adresse, Telefonnummer, Faxnummer, Kontaktformular.	Es ist nur eine oder keine der Kontaktmöglichkeiten angegeben.
	Impressumsangaben: Vertretungsberechtigte bei juristischen Personen	Options-Prüfpunkt	38	PP037	Angabe des Vor- und Nachnamens des Vertretungsberechtigten.	Name des Vertretungsberechtigten wurde unvollständig oder gar nicht angegeben.
	Impressumsangaben: Registereintragung bei juristischen Personen	Options-Prüfpunkt	39	PP038	Angabe der Registriernummer des Handels-/Vereins-/Partnerschafts- oder Genossenschaftsregisters sowie Name und Sitz des zuständigen Amtsgerichts.	Es fehlt eine, mehrere oder alle Angaben der Registernummer oder Name oder Sitz des zuständigen Amtsgerichts.
	Impressumsangaben: Anerkennung bestimmter Berufsgruppen	Options-Prüfpunkt	40	PP039	Pflichtangaben für bestimmte Berufsgruppen und Situationen, welche der Antragssteller im Antrags- bzw. Zuarbeiten-Formulars gemacht hat: a) Die gesetzliche Berufsbezeichnung und der Staat, in dem diese verliehen worden ist. b) Die Bezeichnung der berufsrechtlichen Regelungen und wie diese zugänglich sind. c) Kontaktinformationen zur Kammer, Behörde oder Beschwerdestelle.	Es fehlt eine, mehrere oder alle Angaben von a), b) oder c), obwohl der Antragsteller dazu Angaben im Zuarbeiten-Formular gemacht hat.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
	Impressumsangaben: Internetshops/Verkaufswebseiten	Options-Prüfpunkt Angabe der internationalen Umsatzsteuer-ID	41	PP040	Angabe der internationalen Umsatzsteuer-ID für Webshops und Verkaufsseiten[10], bestehend aus einer fiskalischen Erkennungsnummer, aus der internationalen Länderkennung „DE“ und einer neunstelligen Zahlenfolge. Anhand des Tools "Umsatzsteuer-ID prüfen" (https://ust-id-pruefen.de/) wird erfolgreich geprüft, dass die Umsatzsteuer-ID gültig und aus Deutschland ist.	Die internationale Umsatzsteuer-ID wurde nicht oder nicht vollständig angegeben oder die Prüfung anhand des Tools "Umsatzsteuer-ID prüfen" (https://ust-id-pruefen.de/) ergibt, dass die die Umsatzsteuer-ID nicht gültig oder nicht aus Deutschland ist.
Benutzerfreundlichkeit	Responsives Design: Erkennbarkeit des Inhalts bei mobilen Endgeräten	Mobile Version Responsiv-Test	42	PP041	Das Vorhandensein der Ansicht im Responsive Design wird mit dem Chrome-Browser von Google geprüft. Dafür muss im Chrome-Browser in die mobile, responsive Ansicht in den Entwicklertools gewechselt werden (Menü -> Weitere Tools -> Entwicklertools) und dort eine Displaybreite von 320 Pixeln (obere Leiste; Ansicht "Mobile S") gewählt werden. In der mobilen Ansicht müssen alle Formulare (aus PP017 - PP019), die Datenschutzerklärung und das Impressum, ohne horizontales Scrollen, vollständig sichtbar sein. Texte und Bilder können vereinzelt ohne Limit überstehen, vorausgesetzt,	In der mobilen Ansicht des Chrome Browsers mit 320 Pixeln Displaybreite sind nicht alle vorhandenen Formulare oder die Datenschutzerklärungsseite oder die Impressumsseite ohne horizontales Scrollen vollständig sichtbar oder der gesamte Text oder alle Bilder einer Seite stehen über die Bildschirmbreite über.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					dass nicht der gesamte Text oder alle Bilder einer Seite überstehen. Für diese Prüfung müssen alle Seiten der zu zertifizierenden Webseite und insbesondere die Datenschutzerklärungs-, die Impressumsseite sowie alle Seiten, die Formulare beinhalten, betrachtet werden.	
Globale Zusatzprüfung	Gesetzeskonforme Ausführung der Webseite hinsichtlich der Integrationen, Erweiterungen und Ausführungsart in Bezug auf Cyber-Sicherheit, DSGVO, TMG.	Options-Prüfpunkt	43	PP043	Dieser Prüfpunkt ist dann erforderlich, wenn die Anzahl der Mitarbeiter 50 oder mehr beträgt oder von einem Antragsteller mit weniger als 50 Mitarbeitern explizit beantragt wurde. Es wird geprüft, ob eine Bestätigung vorliegt, die eine fach- und sachgerechte Erstellung aller rechtlich relevanter Pflichtangaben sowie die technische Umsetzung im Sinne der Cyber-Sicherheit, DSGVO, TMG erfordert. Die Webseite muss dafür in allen Bereichen begutachtet werden. Die Begutachtung und die Bestätigung der erfolgreichen Durchführung stellt ein vertrauenswürdiger Gutachter oder Berater, als	Wenn dieser Prüfpunkt erforderlich ist, indem die Anzahl der Mitarbeiter 50 oder mehr beträgt oder von einem Antragsteller mit weniger als 50 Mitarbeitern explizit beantragt wurde. Und wenn die Aufstellung (Liste) nicht mit den “Zuarbeiten” eingereicht wurde oder darauf die fachgerechte Umsetzung vom Gutachter nicht schriftlich bestätigt wurde.

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					unabhängige Person oder Organisation, aus. Dem Gutachter/Berater ist vom Antragsteller nachvollziehbar darzulegen, von welchen Fachkundigen oder Unternehmen (o. ä.) die Ausführungen auf der Webseite erstellt wurden. Sind Umsetzungen auch oder ausschließlich von Mitarbeitern des Antragstellers umgesetzt worden, so kann der Antragsteller die fachgerechte Erstellung formlos versichern, und diese wird anerkannt, wenn der Gutachter sich über die Glaubwürdigkeit und Nachvollziehbarkeit der Versicherung informiert hat und bestätigen kann. Die Grundlage der Versicherung und Bestätigung ist eine Liste mit Angaben aller relevanter rechtlicher und technischer Webseitenbereiche, die für den Zweck der Begutachtung relevant sind. Die Aufstellung (Liste) ist mit den “Zuarbeiten” einzureichen und muss als, “nach vorliegenden	

Prüfbereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID	konform	nicht konform[1]
					Informationen fachgerecht umgesetzt", vom Gutachter auf dem Formular schriftlich bestätigt werden.	

Hinweise und Prüfvorgaben zum Audit – Prüfliste

- Zu Beginn des Audits müssen die Daten und Angaben geprüft bzw. verifiziert werden:
  - Sind die Angaben im Kundendaten-Antragsformular und auf der Webseite einheitlich?
  - Handelt es sich um ein deutsches Unternehmen?
  - Sind die Unternehmensdaten vollständig und nachvollziehbar?
  - Handelt es sich um einen Webshop oder Verkaufsseite?
  - Ist die Basissprache in den zu prüfenden Bereichen Deutsch (ausgenommen zusätzlich englischsprachige Seiten)?
- Nach dem Zustandekommen des Zertifizierungsvertrags und vor dem Audit müssen bestimmte Verifizierungsunterlagen zur Inhaberschaft an den Zertifizierer gesendet werden (s. Prüfbereich Inhaberschaft). Erst wenn diese vollständig sind, kann das Audit erfolgen.
- Für die Prüfung muss der Chrome-Browser in der aktuellsten Form verwendet werden.

[1] Nicht konforme Ergebnisse sind grundsätzlich per Screenshot intern zu dokumentieren und auch dem Antragsteller bei der Begründungsmitteilung zukommen zu lassen. Zur Erstellung von Screenshots Programmhandbuch Anlage 3 Punkt 4 beachten.

[2] Damit bei Verwendung des Chrome-Browsers die vollständige URL inkl. http:// bzw. https:// sichtbar wird, muss auf die URL in der Browser-Adresszeile doppelt geklickt werden.

[3] DSGVO für DE mit Ausführungserweiterungen durch das BDSG (Bundesdatenschutzgesetz) Fassung aus Juni 2019.

[4] HTTP-Cookie auch als Web-Cookie, Internet-Cookie, Browser-Cookie oder einfach als Cookie bezeichnet.

[5] Opt-Out bedeutet einen Widerspruch ausdrücken. Im Fall des Cookie-Hinweises kann man durch den Opt-Out-Button der Verwendung von Cookies widersprechen.

[6] Opt-in bedeutet eine Zustimmung ausdrücken. Im Fall des Cookie-Hinweises kann man durch den Opt-In-Button der Verwendung von Cookies zustimmen.

[7] Kontaktdaten gleich wie Unternehmensdaten im Impressum.

[7a] Als Seiten sind sämtliche Webseiten mit einer eindeutigen URL gemeint.

[8] Ein Formular ist ein Bereich mit Eingabefeldern welche durch Klick auf einen beschrifteten Button versendet werden.

[9] Eingetragene Unternehmensrechtsform dargestellt wie: Einzelunternehmen, GbR, UG, GmbH, gGmbH, KG, eG, AG, e.V., Nebenerwerb, Ltd., Stiftung.

[10] Verkaufsseiten sind Webseiten, auf denen ein Webshop vorhanden ist oder andere entgeltliche Verkäufe, die mit Preisangaben, Bestellverfahren betrieben werden.

5.4.2 IWTS-STANDARD VARIANTE INTERNATIONAL

Prüf-bereich	**Kriterium**	**Erweiterte Hinweise für Kriterium**	**Kriterien-Nr.**	**Kriterien-ID Int.**	**Anlehnung an Kriterien-ID Dtl.**	**konform**	**nicht konform[1]**
Cyber-Sicherheit	URL-Test	Keine offene Weiterleitung auf andere URL nach Aufruf der Betreiber-Webseiten-URL	1	PE001	PP001	Die bei Zertifikatsantrag angegebene URL ändert sich nicht, wenn diese im Browser aufgerufen wird (keine Weiterleitung).	Die bei Zertifikatsantrag angegebene URL ändert sich nach dem Aufruf in einem Browser (Weiterleitung).
	https:// URL	Hypertext Transfer Protocol Secure (HTTPS)	2	PE002	PP002	Die im Browser aufgerufene URL zeigt von vorn beginnend zuerst diese 8 Zeichen: https:// Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Es werden nicht zuerst von vorne oder nicht eindeutig die 8 Zeichen https:// angezeigt.
	SSL/TLS – Secure Sockets Layer/Transport Layer Security Verschlüsselung	Funktionsprüfung SSL-/TLS-Zertifikat Kommunikationsprotokoll Transport Layer Security, starke Verschlüsselung des	3	PE003	PP003	Das SSL-/TLS-Zertifikat wird mit dem Tool "Comodo SSL Checker " (https://comodosslstore.com/ssltools/ssl-checker.php) und dem Tool "SSL Labs SSL Server Test" (https://www.ssllabs.com/ssltest) getestet und das Ergebnis enthält weder Sicherheits- noch Warnhinweise (die Gesamtergebnisse sind grün gekennzeichnet).	Das SSL-/TLS-Zertifikat wird mit dem Tool "Comodo SSL Checker" und dem Tool "SSL Labs SSL Server Test" getestet und das Ergebnis zeigt mindestens einen Sicherheits- oder Warnhinweis an (beide oder eines der Gesamtergebnisse sind rot/orange gekennzeichnet).

Prüf-bereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID Int.	Anlehnung an Kriterien-ID Dtl.	konform	nicht konform[1]
		Kommunikationsprotokolls				Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	
	Technischer Sicherheitstest	Prüfung der Webseite auf aktuell bekannte und relevante schadhafte Systeme, Schadprogramme und Sicherheitslücken (dazu gehören u.a. Malware, Viren, offizielle Blacklists)	4	PE019	PP042	Die Prüfung der Webseite mit dem Prüf-Tool "Sucuri Site Check" (https://sitecheck.sucuri.net/) ergibt im Gesamtergebnis nur ein “minimales” oder höchstens “geringes" Risiko (Low) und ist somit jeweils grün. Ergebnis ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Die Prüfung der Webseite mit dem Prüf-Tool "Sucuri Site Check" ergibt im Gesamtergebnis ein höheres als “geringes Risiko” (Low) und ist somit orange oder rot.
Datenschutz	Web-Kontaktformular/e: Personenbezogene Datenerfassung	Kein pauschales Datensammeln, keine pauschalen Pflichtfelder	5	PE004	PP019	Es werden nur notwendige Daten wie Anrede, Name, E-Mail-Adresse, Betreff und Textnachricht in einem Kontaktformular durch definierte Pflichtfelder abgefragt. Alle anderen abgefragten Daten dürfen keine Pflichtfelder sein. Handelt es sich um eine Newsletter-Anmeldung, darf nur das E-Mail-Feld ein Pflichtfeld sein.	Es werden in einem Kontaktformular über die Daten oder Fragen wie Anrede, Name, E-Mail-Adresse, Betreff, Textnachricht bzw. bei einer Newsletter-Anmeldung über das E-Mail-Feld hinaus weitere Daten abgefragt, die als Pflichtfelder gekennzeichnet sind oder ohne deren Eingabe das Absenden des Formulars/der Anmeldung technisch verhindert wird.

Prüf-bereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID Int.	Anlehnung an Kriterien-ID Dtl.	konform	nicht konform[1]
						Für diese Prüfung müssen alle Seiten[2] der zu zertifizierenden Webseite auf Formulare abgesucht werden.	Für diese Prüfung müssen alle Seiten[2] der zu zertifizierenden Webseite auf Formulare abgesucht werden.
Inhaberschaft	Domain-Inhaberschaft bzw. Nutzungs-Berechtigung	Berechtigung URL-Nutzung Vorab-Dokument	6	PE005	PP025	Der Auftraggeber hat im Zuarbeiten-Formular bestätigt, dass er den Key für die Domain-Inhaber-Verifikation hinterlegt hat und der Auftraggeber hat den ihm im Auftragsprotokoll ausgewiesenen Key in der Form "iwts-site-verification-[Key]" im DNS-Report seines Domain- bzw. Server-Hosters hinterlegt und die Prüfung mit dem Tool Qualidator DNS Report (https://www.qualidator.com/WQM/de/Tools/DNSReport.aspx) bestätigt, dass der Key hinterlegt wurde. Ergebnis des Prüfergebnisses mit dem DNS Report Tool ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Der Auftraggeber hat im DNS-Report seines Domain- bzw. Server-Hosters keinen Key oder einen vom Auftragsprotokoll abweichenden Key hinterlegt.
	Inhaberschaft Verifizierung Registerauszug	Options-Prüfpunkt Vorab-Dokumente[Fehler!]	7	PE006	PP026	Entweder der Antragsteller hat bei der Antragstellung angegeben, dass er Register-eintragspflichtig ist und hat vorab ein Dokument „Registerauszug“ zugesendet. Dann ist zu prüfen, ob die	Entweder der Antragsteller hat bei der Antragstellung angegeben, dass er Register-eintragspflichtig ist, hat aber vorab kein Dokument „Registerauszug“ zugesendet.

Prüf-bereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID Int.	Anlehnung an Kriterien-ID Dtl.	konform	nicht konform[1]
		Textmarke nicht definiert.				Unternehmens-, Inhaber-, Adress- und Registrierungsdaten des Dokuments mit den Angaben auf der zu zertifizierenden Webseite übereinstimmen. Oder der Antragsteller hat bei der Antragstellung angegeben, dass er nicht Register-eintragspflichtig ist.	Oder der Antragsteller hat bei der Antragstellung angegeben, dass er Register-eintragspflichtig ist und hat vorab ein Dokument „Registerauszug“ zugesendet. Die Unternehmens-, Inhaber-, Adress- oder Registrierungsdaten des Dokuments stimmen aber nicht mit den Angaben auf der zu zertifizierenden Webseite überein.
	Inhaberschaft Verifizierung Gewerbeanmeldung	Options-Prüfpunkt Vorab-Dokumente**Fehler! Textmarke nicht definiert.**	8	PE007	PP027	Dieser Prüfpunkt ist nur relevant, wenn der Antragsteller in Prüfpunkt PP026 angegeben hat, dass er nicht Register-eintragspflichtig ist: Entweder der Antragsteller hat bei der Antragstellung angegeben, dass er Gewerbe-anmeldepflichtig ist und hat vorab ein Dokument „Gewerbeanmeldung“ zugesendet. Dann ist zu prüfen, ob die Unternehmens-, Inhaber-, Adress- und Registrierungsdaten des Dokuments mit den Angaben auf der zu zertifizierenden Webseite übereinstimmen. Oder der Antragsteller hat bei der Antragstellung angegeben, dass er nicht Gewerbe-anmeldepflichtig ist.	Dieser Prüfpunkt ist nur relevant, wenn der Antragsteller in Prüfpunkt PP026 angegeben hat, dass er nicht Register-eintragspflichtig ist: Entweder der Antragsteller hat bei der Antragstellung angegeben, dass er Gewerbe-anmeldepflichtig ist, hat aber vorab kein Dokument „Gewerbeanmeldung“ zugesendet. Oder der Antragsteller hat bei der Antragstellung angegeben, dass er Gewerbe-anmeldepflichtig ist und hat vorab ein Dokument „Gewerbeanmeldung“ zugesendet. Die Unternehmens-, Inhaber-, Adress- oder Registrierungsdaten des Dokuments stimmen aber nicht mit den Angaben auf der zu zertifizierenden Webseite überein.

Prüf-bereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID Int.	Anlehnung an Kriterien-ID Dtl.	konform	nicht konform[1]
	Inhaberschaft Verifizierung Rechnungsdokument	Options-Prüfpunkt Vorab-Dokumente**Fehler! Textmarke nicht definiert.**	9	PE008	PP028	Dieser Prüfpunkt ist nur relevant, wenn kein anderes Dokument entsprechend der Prüfpunkte PE006 oder PE007 vorliegt: Es ist zu prüfen, ob ein Dokument "Rechnungsdokument" vorab zugesendet wurde und die Unternehmens-, Inhaber-, Adress-, Registrierungsdaten des Antragstellers mit den Angaben auf der Webseite übereinstimmen.	Dieser Prüfpunkt ist nur relevant, wenn kein anderes Dokument entsprechend der Prüfpunkte PP006 oder PP007 vorliegt: Das Dokument ist nicht vorhanden oder eine oder mehrere Datenangaben sind nicht identisch oder fehlen.
	Impressum: Hinweis	Eindeutige Wahrnehmungsmöglichkeit	10	PE009	PP029	Es wird auf jeder beliebigen Webseite der zu prüfenden Domain, im Header (oben) oder Footer (unten) gut sichtbar ein Link mit der Bezeichnung "Impressum" angezeigt, der auf die Impressumsseite verlinkt. Alternativ können stattdessen auf jeder Seite gut sichtbar die vollständigen Impressumsangaben, wie in den Prüfpunkte PE011 bis PE017 verlangt, dargestellt sein. Ergebnis einer Seite ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Es wird nicht auf jeder beliebigen Webseite der zu prüfenden Domain, im Header (oben) oder Footer (unten) gut sichtbar ein Link mit der Bezeichnung "Impressum" oder die vollständigen Impressumsangaben, wie in den Prüfpunkten PE011 bis PE017 verlangt, angezeigt.

Prüf-bereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID Int.	Anlehnung an Kriterien-ID Dtl.	konform	nicht konform[1]
	Impressum: Weiterleitungs-Link zur Impressumsseite	Link zu Impressumsseite vorhanden	11	PE010	PP030	Bei einem Klick auch den Link "Impressum" muss ein neuer Bereich oder eine neue Seite mit der Kennzeichnung Impressum und dem Impressumsinhalt sichtbar werden. Ergebnis des vollständigen Impressums ist per Screenshot zu dokumentieren (Programmhandbuch Anlage 3 Punkt 4 beachten).	Bei Klick auch den Link "Impressum" sind die Impressumsdaten nicht zu sehen.
	Impressum: Inhaberangaben/Unternehmensauskunft	Pflichtangaben Inhaberdaten	12	PE011	PP031	Die Angaben zu Unternehmensname, Inhaber Vor- und Nachname, Anschrift (Straße, Hausnummer, PLZ, Ort) sind vorhanden.	Es fehlt eine oder mehrere Pflichtangaben zum Unternehmen wie: Unternehmensname, Vor- und Nachname des Inhabers, Anschrift (Straße, Hausnummer, PLZ, Ort).
	Impressum: Eingetragenes Unternehmen	Options-Prüfpunkt Prüfung ob es sich um eine juristische Person handelt	13	PE012	PP033	Dieser Prüfpunkt ist nur relevant, wenn es sich beim Unternehmen der zu prüfenden Webseite um ein eingetragenes Unternehmen handelt, nicht aber bei Einzelunternehmen: Die Angabe des Antragstellers im Zertifizierungsantrag, ob es sich beim Antragsteller um eine eingetragene juristische Person handelt, wurde mit "Ja" beantwortet und ein Registerauszug, den der Antragsteller übermittelt hat, liegt als Dokumentenkopie vor.	Der Antragsteller hat bei Antragstellung angegeben, dass es sich beim Unternehmen um ein eingetragenes Unternehmen (als juristische Person) handelt, es liegt jedoch kein Registerauszug als Dokumentenkopie vor oder der Antragsteller hat bei Antragstellung angegeben, dass es sich beim Unternehmen um kein eingetragenes Unternehmen (als juristische Person) handelt, jedoch lässt die angegebene Unternehmensform im Impressum darauf schließen, dass es sich

Prüf-bereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID Int.	Anlehnung an Kriterien-ID Dtl.	konform	nicht konform[1]
							um ein eingetragenes Unternehmen (als juristische Person) handelt.
	Impressumangaben: Rechtsform des Unternehmens bei juristischer Person	Options-Prüfpunkt	14	PE013	PP034	Bei juristischen Personen muss die Unternehmensrechtsform[9] als Abkürzung oder ausgeschrieben hinter dem Unternehmensnamen stehen.	Beim Unternehmen handelt es sich um eine juristische Person, die Rechtsform steht aber weder abgekürzt noch ausgeschrieben hinter dem Unternehmensnamen.
	Impressumsangaben: Kontaktmöglichkeit 1		15	PE014	PP035	Es muss eine der folgenden Kontaktmöglichkeiten vorhanden sein: E-Mail-Adresse, Telefonnummer, Faxnummer, Kontaktformular.	Es ist keine der folgenden Kontaktmöglichkeiten angegeben: E-Mail-Adresse, Telefonnummer, Faxnummer, Kontaktformular.
	Impressumsangaben: Kontaktmöglichkeit 2		16	PE015	PP036	Es muss eine weitere Kontaktmöglichkeit (ungleich Kontaktmöglichkeit 1) vorhanden sein: E-Mail-Adresse, Telefonnummer, Faxnummer, Kontaktformular.	Es ist nur eine oder keine der Kontaktmöglichkeiten angegeben.
	Impressumsangaben: Vertretungsberechtigte bei juristischen Personen	Options-Prüfpunkt	17	PE016	PP037	Angabe des Vor- und Nachnamens des Vertretungsberechtigten.	Name des Vertretungsberechtigten wurde unvollständig oder gar nicht angegeben.
	Impressumsangaben: Registereintragung bei juristischen Personen	Options-Prüfpunkt	18	PE017	PP038	Angabe der Registriernummer des Handels-/Vereins-/Partnerschafts- oder Genossenschaftsregisters sowie Name und Sitz des zuständigen Amtsgerichts.	Es fehlt eine, mehrere oder alle Angaben der Registernummer oder Name oder Sitz des zuständigen Amtsgerichts.

Prüf-bereich	Kriterium	Erweiterte Hinweise für Kriterium	Kriterien-Nr.	Kriterien-ID Int.	Anlehnung an Kriterien-ID Dtl.	konform	nicht konform[1]
Benutzer-freundlichkeit	Responsives Design: Erkennbarkeit des Inhalts bei mobilen Endgeräten	Mobile Version Responsiv-Test	19	PE018	PP041	Das Vorhandensein der Ansicht im Responsive Design wird mit dem Chrome-Browser von Google geprüft. Dafür muss im Chrome-Browser in die mobile, responsive Ansicht in den Entwicklertools gewechselt werden (Menü -> Weitere Tools -> Entwicklertools) und dort eine Displaybreite von 320 Pixeln (obere Leiste; Ansicht "Mobile S") gewählt werden. In der mobilen Ansicht müssen alle Formulare (aus PE004), die Datenschutzerklärung und das Impressum, ohne horizontales Scrollen, vollständig sichtbar sein. Texte und Bilder können vereinzelt ohne Limit überstehen, vorausgesetzt, dass nicht der gesamte Text oder alle Bilder einer Seite überstehen. Für diese Prüfung müssen alle Seiten der zu zertifizierenden Webseite und insbesondere die Datenschutzerklärungs-, die Impressumsseite sowie alle Seiten, die Formulare beinhalten, betrachtet werden.	In der mobilen Ansicht des Chrome Browsers mit 320 Pixeln Displaybreite sind nicht alle vorhandenen Formulare oder die Datenschutzerklärungsseite oder die Impressumsseite ohne horizontales Scrollen vollständig sichtbar oder der gesamte Text oder alle Bilder einer Seite stehen über die Bildschirmbreite über.

Hinweise und Prüfvorgaben zum Audit – Prüfliste

- Zu Beginn des Audits müssen die Daten und Angaben geprüft bzw. verifiziert werden:
    - Sind die Angaben im Kundendaten-Antragsformular und auf der Webseite einheitlich?
    - Sind die Unternehmensdaten vollständig und nachvollziehbar?
    - Handelt es sich um einen Webshop oder Verkaufsseite?
    - Ist die Basissprache in den zu prüfenden Bereichen Deutsch oder Englisch?
- Nach dem Zustandekommen des Zertifizierungsvertrags und vor dem Audit müssen bestimmte Verifizierungsunterlagen zur Inhaberschaft an den Zertifizierer gesendet werden (s. Prüfbereich Inhaberschaft). Erst wenn diese vollständig sind, kann das Audit erfolgen.
- Für die Prüfung muss der Chrome-Browser in der aktuellsten Form verwendet werden.

1 Nicht konforme Ergebnisse sind grundsätzlich per Screenshot intern zu dokumentieren und auch dem Antragsteller bei der Begründungsmitteilung zukommen zu lassen. Zur Erstellung von Screenshots Programmhandbuch Anlage 3 Punkt 4 beachten.

2 Als Seiten sind sämtliche Webseiten mit einer eindeutigen URL gemeint.

5.5 Vertragspflichten zwischen den Beteiligten

a) Zwischen dem Webseitenbetreiber und der Zertifizierungsstelle ist vor dem ersten Audit ein Vertrag zu schließen. Beide Seiten sind frei in der Gestaltung dieses Vertrages.

Der Vertrag sollte mindestens enthalten:

- Rechte und Pflichten jeder vertragschließenden Seite
- Vorgehen jeder Seite bei festgestellter bei Nichteinhaltung von einzelnen Kriterien des FdWB-Standards durch den Kunden.
- Vorgehen bei Vertragsverletzungen
- Kündigungsklausel
- Vergütungsfestlegung
- Die Nutzung der Schlichtungsstelle (Beirat des FdWB) bevor gerichtliche Schritte unternommen werden.
- Weiterhin alle üblichen formalrechtlichen Vereinbarungen.

Ohne die Vertragsfreiheit einzuschränken, sind folgende Spezifika der Zertifizierung im Vertrag zu berücksichtigen:

- *Zur Kündigungsklausel*: Die Zertifizierungsstelle wird mit Rücksicht auf ihre Pflichten, die sie mit der Anerkennung vom FdWB übernahm den Vertrag üblicherweise nur dann kündigen, wenn der Kunde mehrfach schwere Vertragsverletzungen begangen hat.
  Zertifizierungsanträge von Antragstellern, die mehrere kurzfristige Wechsel der Zertifizierungsstellen vollzogen haben und dafür der Zertifizierungsstelle keine anerkennungsfähige Begründung geben können, können wegen hohen Risikos abgelehnt werden. Falls das genannte Risiko vertuscht wurde, kann die Zertifizierungsstelle jederzeit mit sofortiger Wirkung kündigen.
  Die Zertifizierungsstelle hat das Recht, bei Missbrauch des Zertifikats oder des Konformitätszeichens jederzeit mit sofortiger Wirkung den Vertrag zu kündigen.
  Erfolgte die Kündigung der Vertrages durch die zertifizierungsstelle, weil der Kunde seine Vertragspflichten schuldhaft verletzte, haftet die Zertifizierungsstelle nicht für mögliche Schäden beim gekündigten Unternehmen.
  Mit der gültigen Kündigung des Vertrages erlischt das von der Zertifizierungsstelle vergebene Zertifikat und die Berechtigung zur Verwendung des Logos. Es muss umgehend von der Webseite entfernt werden.
  Die Zertifizierungsstelle meldet dem FdWB die erfolgte Vertragskündigung. Der FdWB veranlasst die Verschiebung in der Zertifikatsliste von „gültige Zertifikate“ in „beendete Zertifikate“.
- Zur *Gebührenordnung*: Die Zertifizierungsstelle legt ihre Gebührenordnung eigenständig fest. Diese soll mindestens folgende Angaben enthalten:
  - Die Gebührenliste gibt die Gebühren für ein Kalenderjahr an für die komplette Durchführung des Zertifizierungsverfahrens, bestehend aus der Durchführung von Audits, Zertifizierungen und weiteren für das Zertifizierungsverfahren speziellen Einzelleistungen.
  - Gebühren für Audits (Erstaudit, Folgeaudit, außerordentliches Audit)
  - Gebühr für Erstellung des Auditberichts
  - Gebühr für Zertifizierung und Zustellung des Zertifikats
  - evtl. weitere Leistungen

  Es ist möglich mehrere oder alle Gebührenelemente zu mehreren Teil-Pauschalen oder einer Gesamtpauschale zusammenzufassen.

  Die Gebührenordnung ist im Antragsverfahren der Zertifizierungsstelle beim Programmträger vorzulegen.

b) Die Regelung der Zusammenarbeit zwischen Zertifizierungsstelle und dem Programmeigner erfolgt durch Anerkennung oder Vertrag.

c) ANMERKUNG: Zwischen dem Zertifizierungskunden und dem Programmeigner entsteht kein Rechtsverhältnis. Es ist aber möglich, dass zwischen diesen beiden Parteien ein anderes Rechtsverhältnis entsteht, z.B. in ihren Eigenschaften als Fachverband und Webseitenbetreiber zur Fachberatung oder zur Verbandsmitgliedschaft usw.

5.6 Voraussetzungen für die Erteilung des Zertifikats

Folgende Voraussetzungen müssen für die Erteilung eines Zertifikats erfüllt sein:

a) Die Zertifizierungsstelle verfügt über eine gültige Akkreditierung durch eine nationale Akkreditierungsstelle sowie eine gültige Zulassung durch den Programmeigner.

b) Sie hat den Zertifizierungsantrag eines Webseitenbetreibers angenommen und es liegt ein Zertifizierungsvertrag mit einem Webseitenbetreiber vor.

c) Ein von der Zertifizierungsstelle anerkannter Auditor hat ein Audit durchgeführt, welches die Konformität mit den Webseitenkriterien und den Zertifizierungsvorschriften ergab.

d) Nach dem Vier-Augenprinzip hat ein von der Zertifizierungsstelle anerkannter Zertifizierer die Zertifizierungsentscheidung getroffen.

e) Das Zertifikat muss mindestens folgende Angaben enthalten:
   - Name der Zertifizierungsstelle
   - Name des zertifizierten Programms (Falls das Programm mehrere Qualitätsstufen unterscheidet, die zutreffende Qualitätsstufe.)
   - Konformitätszeichen (Falls nationale oder regionale Versionen des Programms angewendet werden ist das jeweils zutreffende Zeichen zu verwenden)
   - Zertifizierungsdatum
   - Unterschrift des Zertifizierers
   - Zulässig ist die Verwendung des Konformitätszeichens (Logo)

5.7 Nichtkonformität zum FdWB-Standard

Nichtkonformität kann verschiedene Gründe haben, z.B.

a) der Kunde hat versäumt beim Aufbau oder der Veränderung seiner Webseite die Konformität zu allen Kriterien des FdWB-Standards herzustellen,
b) der Kunde hat versäumt, alle Eigenschaften seiner Webseite an Veränderungen des FdWB-Standards anzupassen,
c) der Kunde hat durch Manipulationen den Eindruck erweckt, seine Webseite sei konform,
d) durch Verschulden des Kunden ist die Rezertifizierung nicht (rechtzeitig) erfolgt.

Wird durch ein Audit oder durch Beschwerden Dritter über die Nichtkonformität der Webseite oder durch Überwachung oder auf anderem Wege die Nichtkonformität festgestellt, erfolgen folgende Maßnahmen durch die Zertifizierungsstelle:

a) Der Kunde wird im Audit mündlich durch den Auditor ansonsten schriftlich durch die Zertifizierungsstelle über die Abweichung informiert.
b) Unabhängig vom Grund der Abweichung hat der Kunde das Logo von der Webseite umgehend zu entfernen.
c) Bei geringfügiger Abweichung oder bei geringem Risiko der Abweichung stellt die Zertifizierungsstelle dem Kunden eine Frist zur Herstellung der Konformität. Diese Frist soll angemessen sein, die Abweichung selbst oder durch Hinzuziehung Dritter zu korrigieren.
   Nach der Meldung der Herstellung durch den Kunden an die Zertifizierungsstelle erfolgt ein außerplanmäßiges Audit zur Feststellung der Konformität. Ist diese festgestellt, darf das logo erneut auf der Webseite angebracht werden.

d) Bei erheblichen Abweichungen oder großem Risiko oder wird wie bei c) verfahren. Jedoch kann die Zertifizierungsstelle befristet das Zertifikat als ungültig erklären oder entziehen. Die Wiederherstellung der Gültigkeit erfolgt durch schriftliche Mitteilung an den Kunden. Nach dem Entzug ist ein erneutes Erstaudit erforderlich, das Zertifikat wiederzuerlangen.
e) Bei sehr erheblichen Abweichungen oder bei der Weigerung des Kunden die Konformität wiederherzustellen, kann der Programmeigner über die „Liste der Zertifikate“ die Öffentlichkeit über den Zertifikatsentzug unterrichten. Geschah der Entzug durch schweren Betrug kann der Programmeigner auch den Grund des Entzugs veröffentlichen.

5.8 Überwachung

Falls erforderlich kann der Programmeigner die „Überwachung“ im Sinne der ISO ISO/IEC 17000:2004, 6.1 bzw. der ISO ISO/IEC 17067:2013, 5.3.7 Programmtyp 5 kurzfristig anordnen. Dafür stehen ihm drei Wege offen:

a) durch Erweiterung des vorliegenden IWTS-Programms oder
b) durch Ermächtigung einzelne oder alle anerkannten Zertifizierungsstellen auf der Grundlage der erfolgten Anerkennung zu beauftragen, eigene Programme zur Überwachung aller Zertifikatsnutzer zu entwickeln, dem Beirat zur Bestätigung vorzulegen und anzuwenden oder
c) durch Ermächtigung einzelner oder alle anerkannten Zertifizierungsstellen auf der Grundlage der erfolgten Anerkennung zu beauftragen, eigene Programme zur Überwachung von Zertifikatsnutzern mit erhöhter Risikostufe zu entwickeln, dem Beirat zur Bestätigung vorzulegen und anzuwenden.

Die Überwachung darf erst beginnen nachdem entschieden wurde welche der Methoden a) bis c) angewendet wird und die dafür erforderlichen Dokumente vom Beirat beschlossen worden sind.

ANMERKUNG: Überwachung bedeutet systematische Wiederholung von Konformitätsbewertungstätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit der Aussage zur Konformität. Wenn Überwachung eingeschlossen ist, sollte das IWTS-Programm den Satz an Tätigkeiten (gemäß ISO/IEC 17067:2013 , Tabelle 1, Funktion 6) festlegen, der Bestandteil der Überwachungsfunktionen ist. Bei der Entscheidung über die geeigneten Überwachungstätigkeiten sollte der Programmeigner die Art des Produkts, die Folgen und die Wahrscheinlichkeit nichtkonformer Produkte sowie die Häufigkeit der Tätigkeiten berücksichtigen.

5.9 Gewährleistung von Transparenz auf allen Ebenen

Auf allen Ebenen des IWTS-Zertifizierungsprogramms wird Transparenz gewährleistet.

Hierzu stellen die Beteiligten alle für die Gewährleistung der Funktion des Systems erforderlichen Informationen den anderen hierfür berechtigten Beteiligten frei zur Verfügung.

Darüber hinaus sorgt der Programmeigner mit seinen Informationen in der Öffentlichkeit dafür, dass auch die Öffentlichkeit und mögliche weitere Interessenten transparent über das IWTS-Programm informiert werden und sein Ruf als beispielhaft gutes System zur Websicherheit jederzeit gefördert wird.

5.10 Widerspruchs- und Schlichtungsverfahren

Zertifizierte Unternehmen und solche Unternehmen, die einen Antrag auf Zertifizierung gestellt haben, können dann, wenn mit dem Beschwerdeverfahren der Zertifizierungsstelle keine Einigung erreicht werden kann, gegen die Zertifizierungsstelle beim Beirat des FdWB, als Schlichtungsstelle, eine Beschwerde gegen folgende Entscheidungen einlegen:

a) Verweigerung des Vertragsabschlusses zum Zertifizierungsverfahren,
b) Anordnung von zusätzlichen Audits,
c) Anordnung von häufigeren Audits im Zusammenhang mit höherer Risikoeinstufung,
d) Verweigerung der Zertifizierung,
e) Entzug des Zertifikats.

Die Beschwerde ist unter Angabe der Gründe einzureichen, in welchen Rechten sich das Beschwerde führende Unternehmen verletzt sieht.

Der Beirat entscheidet innerhalb von zwei Wochen über die Zulässigkeit der Beschwerde. Personen, die direkt von der Entscheidung betroffen sind, werden nicht am Entscheidungsprozess beteiligt.

Gemäß Kapitel 5.5 dieses Handbuchs soll der Beirat als Schlichtungsstelle angerufen worden sein und entschieden haben, bevor gerichtliche Schritte gegangen werden.

Der Beirat schlichtet auch bei Unstimmigkeiten hinsichtlich der Interpretation im IWTS-Programm.

5.11 Aufbewahrung von Aufzeichnungen

Alle Teilnehmer am Programm IWTS haben die Pflicht, die Unterlagen, welche sie zu führen haben auch zu archivieren. Hierbei gelten insbesondere folgende Pflichten:

a) Der ***Programmeigner*** archiviert sämtliche Versionen seines Programms für mindestens 10 Jahre, Dies gilt auch für die Dokumentation der „Programmanpassungen“ (Anlage 1).
b) Die ***Zertifizierungsstellen*** archivieren
   i. alle relevanten Unterlagen zur *Akkreditierung* und *Anerkennungen* von Programmeignern mindestens 5 Jahre,
   ii. alle Dokumente zu *Kundenbeziehungen* (Antragsformular, Vertrag, Auditunterlagen, inkl. Schriftverkehr zu Abweichungen und Zahlungsversäumnissen, Zertifikate) usw. für 3 Jahre. Im Falle von Kündigungen werden die Unterlagen bis zu 3 Jahren nach dem Kündigungsdatum archiviert.

Die Beseitigung archivierter Unterlagen bzw. die Löschung digitaler Speicher hat unter Beachtung der Vorschriften zum Informationsfluss und zur Geheimhaltung sowie der durch Gesetz vorgegebenen Regelungen zu erfolgen.

5.12 Vermarktung des Programms

Die Vermarktung des Programms IWTS erfolgt in Verantwortung des Programmeigners. Ihm stehen dafür alle üblichen Vermarktungswege zur freien Verfügung.

Der Programmeigner gibt den anerkannten Zertifizierungsstellen die Genehmigung, auf allen ihren üblichen Kanälen in der Öffentlichkeit darauf hinzuweisen, dass sie für die Zertifizierung des Programms IWTS tätig sind.

Programmträger und jede einzelne Zertifizierungsstelle werden sich zu ihren Vermarktungsaktivitäten so abstimmen, dass die Vermarktung des Programms optimiert ist.

Gegen das Programm IWTS zertifizierte Kunden dürfen im Rahmen ihrer Interessen die Vermarktung des Programms IWTS unterstützen.

5.13 Informationsfluss und Geheimhaltung

Bis auf die unten genannten Ausnahmen sind sämtliche Daten und Informationen, die im Zertifizierungsprozess ausgetauscht werden vertraulich zu behandeln. Das heißt,

- digital weitergegebene Daten und Informationen,
- auf Papier und anderen Medien gespeicherte Daten und Informationen sowie
- mündlich weitergegebene Informationen

müssen geschützt werden.

Für digitale Daten heißt dies, dass nur gesicherte Datenträger und gesicherte Datenübermittlungsverfahren angewendet werden dürfen. Büroräume und andere Räume in denen vertrauliche Daten aufbewahrt werden sind technisch zu sichern. Der Zugang von unbefugten Personen zu diesen Räumen ist auszuschließen. Durch die am IWTS-Programm Beteiligten sind, wo nötig, durch entsprechende Vereinbarungen zum Datenschutz zu treffen, die auch die Schadensregelungen beinhalten. Der Programmeigner übernimmt keine Gewährleistungsansprüche für entsprechende Schäden.

Die Vernichtung von nicht mehr archivierungsbedürftigen Akten und gleichgestellten digitalen Dateien hat so zu erfolgen, dass Geheimnisse nicht offengelegt werden können.

Ausgenommen von der Geheimhaltung ist die Veröffentlichung von

- Verwendern gefälschter Zertifikate und
- Verwendern abgelaufener oder entzogener Zertifikate.

Informationen über diese ungültigen Zertifikate werden in einer gesonderten Rubrik aller IWTS-Zertifikate im Internet veröffentlicht.

5.14 Verbesserungsvorschläge

Alle beteiligten am IWTS-Programm sind aufgerufen, Verbesserungsvorschläge an den Programmeigner mitzuteilen, die sich aus der praktischen Anwendung ergeben. Der Beirat wird diese Vorschläge bewerten und entscheiden was umgesetzt wird. Es besteht kein Anspruch darauf, dass eingereichte Vorschläge umgesetzt werden.

5.15 Schutzrechte

Die Rechte für die Wort-Bild-Marke des IWTS-Zertifizierungsprogramms liegen beim FdWB.

6 Aufgaben und Verantwortlichkeiten der Beteiligten

6.1 Aufgaben und Verantwortlichkeiten der zertifizierten Unternehmen

6.1.1 Herstellung und Erhalt konformer Webseite

Der Kunde ist selbst dafür verantwortlich, dass seine Webseite jederzeit konform mit dem IWTS-Standard (Kapitel 4.2 dieses Handbuchs) ist.

In Vorbereitung auf das erste Audit sollte der Interessent sich Informationen über die Anforderungen des IWTS-Standards für seine Webseite informieren und durch eine Eigenprüfung den Konformitätsgrad feststellen. Bei noch bestehenden Abweichungen sollte er diese vor dem Audit beseitigen (lassen). Hierzu kann er Beratung Dritter in Anspruch nehmen.

Während des ersten Audits ist der Interessent allein verantwortlich für die volle Konformität aller Produktanforderungen (Kapitel 5.4) und Zertifizierungsanforderungen (Kapitel 5.5 bis 5.15 sowie im Vertrag mit der Zertifizierungsgesellschaft). Festgestellte Defizite gehen, unabhängig von den Ursachen des Mangels, allein zu seinen Lasten. Dies kann auch dazu führen, dass er Nacharbeiten leisten muss und die Erteilung des Zertifikats so lange ausgesetzt wird, bis die Nacharbeiten zur völligen Konformität führten.

Während der Webseitenbetreiber im Besitz eines gültigen Zertifikats ist, hat er eigenverantwortlich dafür zu sorgen, dass die Konformität mit den Anforderungen des IWTS-Programms immer gegeben ist. Dazu gehört auch, dass er sich selbst über ggf. Veränderungen an den Kriterien informieren und dies auf seiner Webseite umsetzen muss.

Der Zertifikatsnutzer ist verpflichtet, Veränderungen an seiner Webseite oder in seinem Unternehmen, die die Konformität zu den Programm-Kriterien betreffen können, unverzüglich der Zertifizierungsstelle, mit der er vertraglich gebunden ist, mitzuteilen.

Dem Zertifikatsnutzer wird empfohlen, für den Fall, dass seine Webseite durch besondere Umstände plötzlich und nicht nur ganz kurzfristig die Konformität nicht gewährleistet, das Logo für diese Zeit von der Webseite zu entfernen, um evtl. Schäden bei Dritten zu vermeiden.

Der Webseitenbetreiber wird nach Aussetzung oder Entzug des Zertifikats seine Bestandskunden schriftlich über den Entzug informieren, um sicherzustellen, dass keine Schäden bei Dritten entstehen können.

Der Webseitenbetreiber gewährt dem Auditor zum vereinbarten Audittermin Zugang zur Webseite, um alle Kriterien des FdWB-Standards auf Konformität prüfen zu können. Verweigerungen des Zugangs, die zu einem neuen Audittermin führen und damit Sonderkosten verursachen, können auf den Webseitenbetreiber umgelegt werden.

Der Webseitenbetreiber gewährleistet, dass er selbst bzw. ein verantwortlicher Mitarbeiter dem Auditor für Rückfragen zum Auditergebnis zur Verfügung steht.

Der Webseitenbetreiber ist verpflichtet, beim Audit festgestellte Abweichungen und Defizite in der Frist zu beseitigen oder beseitigen zu lassen, die von der Zertifizierungsstelle festgelegt wurden und die Zertifizierungsstelle über die Erledigung in Kenntnis zu setzen.

Der Webseitenbetreiber bewahrt alle Kontrollunterlagen mindestens 5 Jahre auf. Er gewährt der Zertifizierungsstelle jederzeit Einsicht in zurückliegende Unterlagen und räumt dem FdWB oder seinen Organen die gleichen Rechte ein wie der Zertifizierungsstelle.

Der Webseitenbetreiber hat das Recht, einen Auditor oder ein Audit abzulehnen, wenn er begründen kann, dass er die in diesem Handbuch geforderten Kriterien zur Objektivität, Neutralität und Unvoreingenommenheit und/oder die Verpflichtung zur Verschwiegenheit vom Auditor oder der Zertifizierungsstelle als nicht gesichert beurteilt. Dazu ist er ebenfalls berechtigt, wenn der den Verdacht hat, dass das Kontrollverfahren nicht ordnungsgemäß durchgeführt wurde. Über diese Ablehnung hat er den Kontrollstellenleiter schriftlich zu informieren.

Der Webseitenbetreiber hat das Recht bei Fragen, Anregungen, Beschwerden, Einsprüchen und Streitfällen zum Zertifizierungsverfahren das Lenkungsgremium der Zertifizierungsstelle anzurufen.

Der Webseitenbetreiber hat das Recht, im Falle einer nicht ordnungsgemäß bearbeiteten Beschwerde an die Zertifizierungsstelle eine Beschwerde an die Schiedsstelle des FdWB einzureichen.

Alle Informationen die im Zertifizierungsverfahren zwischen dem Unternehmen, der Kontrollstelle und dem Verband benötigt werden, werden nur an die zuständigen Verbandsorgane weitergeleitet.

6.1.2 Antrag an Zertifizierungsstelle

Interessierte Webseitenbetreiber stellen einen formgebundenen Antrag (Anlage 2) auf Zertifizierung an eine vom Programmeigner anerkennte Zertifizierungsstelle. Dieser ist erhältlich bei den anerkannten Zertifizierungsstellen. Mit der Bewilligung des Antrags und der Unterzeichnung eines Zertifizierungsvertrages zwischen Kunde (Auftraggeber) und Zertifizierungsstelle sind alle rechtlichen Voraussetzungen für das Zertifizierungsprozesses gelegt.

6.1.3 Gebühren für das Zertifizierungsverfahren

Jede Zertifizierungsstelle erstellt eine eigene Gebührentabelle für Ihre Dienstleistungen gegenüber ihren Kunden (=Webseitenbetreiber). Das Programmhandbuch gibt einen Rahmen für die Gebührentabellen der Zertifizierungsstellen vor. Im Streitfall ist ausschließlich der zwischen Auftraggeber und Zertifizierungsstelle abgeschlossene Vertrag maßgebend.

Die Gebührentabelle sollte mindestens enthalten:

a) Der Auftraggeber verpflichtet sich, sämtliche Kosten, die im Zusammenhang mit den Zertifizierungsverfahren stehen, auf der Grundlage der Gebührenordnung, die in ihrer jeweils gültigen Fassung Bestandteil des Vertrages ist, gemäß den Rechnungen der Zertifizierungsstelle zu vergüten.

b) Die Erhebung von Gebühren erfolgt für alle Zertifizierungstätigkeiten in Abhängigkeit vom tatsächlichen Aufwand. Grundlage für die Bemessung der Gebühren sind

   i. der Aufwand für die Audits und die Zertifizierung,

   ii. die Einstufung des Unternehmens in Größen/Umsatzklassen,

   iii. Reisetage und -kosten: Die Zertifizierungsstellen sind dazu angehalten, derartige Kosten zu reduzieren und zwischen Kunden im gleichen geographischen Gebiet zu teilen, d.h.

sie sind angehalten, Vor-Ort-Besuche bei Kunden in einem geographischen Gebiet möglichst zusammenzulegen und die Kosten aufzuteilen.

iv. Pauschalen für mit der Zertifizierung direkt verbundene Dienstleistungen.

c) Der Kunde erhält eine Rechnung über die erbrachte Leistung. Die Zahlungen sind ohne Abzug binnen 2 Wochen auf das Im Vertrag angegebene Konto der Zertifizierungsstelle zu leisten.

d) Bei verzögerter Bezahlung kann die Zertifizierungsstelle nach der 2. Mahnung das Zertifikat aussetzen. Der Kunde hat dann bis zur Wiedererteilung eines gültigen Zertifikats das Logo von seiner Webseite zu entfernen.

e) Die Zertifizierungsstelle darf einseitig die Gebühren anpassen, wenn sich Umfang oder Ort der Aktivitäten während des laufenden Kalenderjahres ändern. Registrierte Unternehmen sind verpflichtet, jede betriebliche Veränderung, die Einfluss auf die Einhaltung der Kriterien des Standards hat, der zertifizierungsstelle mitzuteilen.

Zur Einsparung von Verwaltungskosten müssen die Zertifizierungsstellen möglicherweise entstehende Gebühren des Programmeigners (z.B. Lizenzen o.ä.) mit der Zertifizierungsrechnung kassieren und an den Programmeigner abführen. Alle zusätzlichen Absprachen werden Teil des Anerkennungsvertrags.

6.1.4 Mitteilung Wesentlicher Änderungen der Webseite

Der Kunde ist verpflichtet, der Zertifizierungsstelle umgehend Mitteilung darüber zu machen, wenn an der zertifizierten Webseite wesentliche Veränderungen vorgenommen wurden, die zu einer Nichtkonformität mit dem erteilten Zertifikat führen könnten.

Stellt sich durch bestimmte Umstände heraus (z.B. Meldungen von Webseitennutzern oder von Wettbewerbern oder durch Überwachung), dass jemand durch die ausgebliebene Meldung einen Schaden erlitten hat, so ist der Kunde dafür allein verantwortlich.

6.1.5 Nutzung des Konformitätszeichens

Zertifizierte Webseitenbetreiber erhalten das Recht, das Konformitätszeichen (Logo) kostenlos auf ihrer Webseite anzubringen, um damit den kaufmännischen Mehrwert ihrer Webseite deutlich und einfach erkennbar den Nutzern ihrer Webseite mitzuteilen. Zertifikatsnutzer dürfen auch weitere ihrer Dokumente, die einen Bezug zum Zertifikat haben, mit dem Logo zu kennzeichnen.
Anmerkung: Es ist für Zertifikatsnutzer nicht erlaubt, das Logo in Zusammenhängen zu benutzen, die keine direkte Verbindung mit der zertifizierten Webseite haben. Beispiel: Ein Maschinenbauunternehmen, dessen Webseite nach dem YXZ-Programm erfolgreich zertifiziert wurde, darf das Logo nicht auf seinem Briefpapier und auf Werbematerialien seiner Erzeugnisse anbringen.

Sobald das Zertifikat ungültig wurde, (egal aus welchem Grund), muss der Zertifikatsnutzer das Logo von seiner Webseite löschen und darf Dokumente, die mit dem Logo gekennzeichnet sind nicht mehr verbreiten.

Der Programmeigner darf Zertifizierungsstellen, deren Webseite eine gleichartige Prüfung wie ein IWTS erfolgreich bestanden hat, die Erlaubnis erteilen, die Webseite der Zertifizierungsstelle mit dem Logo zu markieren.

Die Zertifizierungsstellen, dürfen die Stellen Ihrer Webseiten, die mit dem IWTS-Programm in Verbindung stehen sowie alle vergleichbaren Dokumente kostenlos mit dem Logo markieren.

Der Programmeigner, der gleichzeitig der Rechteinhaber am Logo ist, darf das Logo für seine Zwecke beliebig nutzen.

6.1.6 Transparenz

Zertifikatsinhaber tragen auf zwei Ebenen zur Transparenz des IWTS-Programms aktiv teil:

a) Sie nutzen alle im System existierenden Informationsmöglichkeiten, um jederzeit so über die Zertifizierungsanforderungen an ihre Webseite informiert zu sein, dass Abweichungen vom FdWB-Standard vermieden werden.

b) Sie stellen der Zertifizierungsstelle zum Bedarfszeitpunkt sämtliche Informationen frei und kontrollfähig zur Verfügung, so dass die Zertifizierungsstelle die Konformität mit dem Programm ungehindert feststellen kann.

6.1.7 KÜNDIGUNG

Der Zertifikatsinhaber hat jederzeit die Möglichkeit, seine Teilnahme am IWTS-Zertifizierungsprogramm bei der Zertifizierungsstelle zu kündigen. Ausstehende Zahlungen an die Zertifizierungsstelle sind trotz Kündigung zu begleichen.

6.2 Aufgaben und Verantwortlichkeiten der Zertifizierungsstellen

6.2.1 ANERKENNUNGSVORAUSSETZUNGEN

Die Zertifizierungsstelle muss über eine Reihe von organisatorischen, fachlichen und rechtlichen Voraussetzungen verfügen, um auf Antrag an den Programmeigner von diesem als Zertifizierungsstelle für das IWTS-Programm anerkannt zu werden. Insbesondere sind dies:

a) Erfüllung der Anforderungen an Konformitätsbewertungsstellen gemäß ISIO 17065, welche durch gültige Akkreditierung bei einer nationalen Akkreditierungsstelle bestätigt sind,
b) Anwendung eines Qualitätsmanagementhandbuchs („Verfahrenshandbuch“), welches die Prozesse beschreibt, die die Zertifizierungsstelle durchführt, um konform zur ISO 17065 tätig zu sein,
c) ein auf die Zertifizierungsstelle bezogenes Programmhandbuch, welches die Prozesse beschreibt, die die Zertifizierungsstelle durchführt, um konform zum Programmhandbuch des FdWB tätig zu sein,
d) Regeln für die ständige Gewährleistung der Fachkenntnisse des Personals, das für das IWTS-Programm in der Zertifizierungsstelle tätig ist (Kompetenzerwerb und Kompetenzerhalt),
e) Regeln für die ständige Gewährleistung der persönlichen Voraussetzungen des Personals, das für das IWTS-Programm in der Zertifizierungsstelle tätig ist (Neutralität, Unabhängigkeit, Fähigkeit risikoorientiert in Stresssituationen mit Kunden zu arbeiten),
f) handlungsfähiges Management,
g) gesicherte Büroräume, die auch sichere Gewähr für Daten- und Geheimnisschutz bieten,
h) finanzielle Ressourcen, die die Gewähr bieten, die Zertifizierungstätigkeit für die vertraglich gebundenen Kunden dauerhaft und zuverlässig zu erfüllen.

6.2.2 ZERTIFIZIERUNGSANTRAG INTERESSIERTER WEBSEITENBETREIBER

Webseitenbetreiber, die sich gegen das IWTS-Programm zertifizieren lassen möchten, stellen gemäß der entsprechenden Vorschrift der ISO 17065 bei einer für dieses Programm anerkannten Zertifizierungsstelle einen entsprechenden formgebundenen Antrag (Antragsmuster als Anlage 2).

6.2.3 AUDITDURCHFÜHRUNG

Audits werden durchgeführt zur Feststellung der Konformität der Webseite eines Kunden mit dem IWTS-Programm.

In jedem regulären Audit muss die Konformität ***aller*** Kriterien des aktuell geltenden FdWB-Standards vollständig überprüft werden. Abweichungen sind einzeln zu dokumentieren:

- Welches Kriterium ist nicht konform? Nennung der Kriterien-Nr. des FdWB-Standards.).
- Welche Art der Abweichung wurde festgestellt?
- Frist bis zur Beseitigung der Abweichung durch den Kunden.

Audits können durchgeführt werden durch

1. Einen von der Zertifizierungsstelle anerkannten Auditor für das IWTS-Programm

oder

2. durch geeignete technische Mittel

oder

3. durch eine Kombination von a) und b).

In jedem Fall sind die Anforderungen an Neutralität, Unabhängigkeit und Qualität der Prüfung und Bewertung zu erfüllen, wie sie in ISO 17000, ISO 17065, ISO 17067 und ISO 19011 benannt sind.

Nicht reguläre Audits können jederzeit durchgeführt werden, wenn die Zertifizierungsstelle einen begründeten Verdacht auf Unregelmäßigkeiten hat. Diese sind immer unter Benennung der Verdachtsgründe im Unternehmen anzumelden.

6.2.4 Durchführung der Zertifizierung (Audit, Zertifizierung, Abweichungen, Gültigkeit)

Die Zertifizierung wird durchgeführt durch einen von der Zertifizierungsgesellschaft anerkannten Zertifizierer. Er muss bei seiner Entscheidung berücksichtigen:

a) die durch das Audit festzustellende Konformität der auditierten Webseite mit allen Kriterien des FdWB-Standards,
b) die durch den Zertifizierer festzustellende Konformität mit den Anforderungen des Zertifizierungsprogramms,
c) die durch den Zertifizierer festzustellende Konformität mit den Anforderungen der Zertifizierungsstelle.

Sind alle Anforderungen konform wird das Zertifikat durch den Zertifizierer erteilt und durch Ausfertigung der Zertifikatsurkunde dokumentiert.

Sind einzelne Anforderungen aus a) bis c) nicht konform, muss der Zertifizierer dem Kunden unter Nennung der festgestellten Abweichungen Fristen zur Herstellung der Konformität einräumen. In einfachen Fällen kann die erfolgreiche Beseitigung der Abweichungen durch den Zertifizierer festgestellt werden, was dann zur Zertifikatserteilung führt.
In komplizierten Fällen kann ein weiteres Audit erforderlich werden, die Konformität festzustellen und das Zertifikat durch den Zertifizierer zu erteilen.

So lange nicht alle Anforderungen von a) bis c) komplett erfüllt sind, kann kein Zertifikat erteilt werden.

Das Zertifikat ist gültig

a) bis zum nächsten regulären Audit, i.d.R. 12 Monate,
b) bis zur festgestellten Nichtkonformität, z.B. durch Beschwerden Dritter oder durch außerordentliche Audits infolge der Risikostufe oder entsprechenden Ergebnissen der Überwachung (falls Überwachung durch den Programmeigner angeordnet ist (Kapitel 5.8),
c) beim Entzug des Zertifikats durch die Zertifizierungsstelle,
d) beim Wirksamwerden der Kündigung des Zertifizierungsvertrages.

6.2.5 Regelmäßige und außerordentliche Prüfungen

Grundsätzlich sollen die Webseiten aller Kunden regelmäßig im Jahresrhythmus (alle 12 Monate) durch ein Audit geprüft werden.

Hiervon können durch die Zertifizierungsstelle bei von ihr selbst festgestellter Situation folgende Abweichungen vollzogen werden:

- Die Webseiten einzelner Kunden können, z.B. nach der Beseitigung im Audit festgestellter Abweichungen, einmalig zusätzlich geprüft werden, um den Erfolg der Beseitigung festzustellen. Im Bedarfsfall dürfen so viele einmalige zusätzliche Audits erfolgen bis die Herstellung der Konformität nachgewiesen ist.
- Die Webseiten einzelner Kunden können zusätzlich zum Jahresrhythmus geprüft werden, falls es zu dieser Webseite von Dritter Stelle Mitteilungen an die Zertifizierungsstelle gibt, die Webseite sei nicht konform.
- Wenn durch Änderung gesetzliche Bestimmungen oder durch Änderung von Normen bestimmte Kriterien des FdWB-Standards so geändert worden sind, dass die Umsetzung vor dem nächsten Audit wirksam sein muss, können für alle betroffenen Webseiten zusätzliche Audits nach Wirksamwerden der Standardänderung durchgeführt werden.

- Einzelne zusätzliche Audits können auch dann angeordnet werden, wenn bestimmte Risiken für die Nutzer dieser Webseite entstehen könnten.

Der Vertrag zwischen Zertifizierungsstelle und Kunde ist so abzuschließen, dass der Kunde für alle Kosten aller Audits aufkommen muss. Hat ein Kunde den Eindruck bestimmte Audits sind von der Zertifizierungsstelle fehlerhaft angeordnet oder durchgeführt worden, so hat er hiergegen das Beschwerderecht (Kap. 5.10).

6.2.6 Gewährleistung der Transparenz

Die Zertifizierungsstellen gewährleisten für die Kunden freie Transparenz zu den Grundlagen und den Funktionen des IWTS-Zertifizierungsprogramms sowie zur Anwendung durch den Kunden.

6.2.7 Entzug der Zertifizierung

Bei schwerwiegenden Verstößen gegen die Vorschriften dieses Programmhandbuchs oder gegen den Zertifizierungsvertrag mit der Zertifizierungsstelle kann dem Kunden das Zertifikat von der Zertifizierungsstelle entzogen werden. Vor dem Entzug ist der betroffene Kunde anzuhören. Ist er innerhalb 6 Tagen dazu nicht in der Lage, erfolgt der Entzug dann sofort. Ein rückwirkender Entzug eines Zertifikates ist nicht möglich.

Der Kunde hat unmittelbar nach dem Entzug das Logo des IWTS-Programms von seiner Webseite zu entfernen.

Treten beim Unternehmen, dem das Zertifikat entzogen wurde, durch den Entzug wirtschaftliche oder andere Schäden auf, haftet die Zertifizierungsstelle dafür nur dann, wenn sie schuldhaft ihre Pflichten verletzte. Die maximale Schadenssumme wird auf das 10-fache der jährlichen Zertifizierungsgebühr begrenzt.

Entstehen durch den Zertifikatsentzug Schäden bei Dritten, z.B. Kunden des zertifizierten Unternehmens, haftet dafür der Webseitenbetreiber, dem das Zertifikat vorschriftskonform entzogen wurde.

6.2.8 Berichtspflichten an den Programmeigner

Der Programmeigner hat das Recht, von den anerkannten Zertifizierungsstellen bestimmte Berichte über zur Funktion des Zertifizierungsverfahrens anzufordern, z.B. Neukundengewinnung, Kündigungen, Anzahl vergebener Zertifikate, Anzahl von Abweichungen, Anzahl von Beschwerden u.ä.). Der berichtsumfang soll auf das zur Funktion des Systems erforderliche Mindestmaß begrenzt werden. Die Berichtspflichten werden im Anerkennungsverfahren definiert und im Anerkennungsschreiben dokumentiert.

6.3 Aufgaben *und Verantwortlichkeiten* des Programmeigners

6.3.1 Öffentlichkeitsarbeit

Der Programmeigner wird regelmäßig eine qualifizierte Öffentlichkeitsarbeit für das IWTS-Programm durchführen. Er nutzt dafür seine Webseite, Flyer, Veranstaltungen und weitere geeignete Medien und Formen. Er bezieht dabei alle geografischen Gebiete ein, in denen Zertifizierungsstellen tätig sind.

Der Programmeigner realisiert eine öffentliche Kommunikation, um sein Programm bekannt zu machen und dessen Nutzung zu befördern.

Dabei werden mindestens zwei Zielgruppen gebildet und zielgruppenspezifisch informiert (Separierung der Zielgruppen auf der Programm-Webseite):

a) Allgemein an der Webseitenzertifizierung interessierte Öffentlichkeit. Hierzu können auch Webseitenbetreiber als zugeordnet gesehen werden, solange sie sich noch nicht im Zertifizierungsprozess befinden. Der Inhalt konzentriert sich auf Aufklärung über den Nutzen des

Zertifizierungsprogramms und sein Zertifikat. Das Informationsangebot ist relativ statisch. Medien sind z.B. Programm-Webseite, Broschüren, öffentliche Konferenzen usw.

b) Nutzer des Zertifizierungsprogramms. Hierzu zählen die Zertifikatsnutzer und Zertifizierungsstellen. Der Inhalt konzentriert sich auf die praktischen Anwendungsthemen. Das Informationsangebot muss sehr rasch auf Neuigkeiten zum Programm und seinem gesellschaftlichen Umfeld reagieren und flexibel sein. Medien sind z.B. Programm-Webseite, Newsletter, Beratungsangebot.

Der Programmeigner wird die anerkannten Zertifizierungsstellen im rechtzeitig im Vorab über besondere Aktionen unterrichten, so dass diese vorbereitet sind, ggf. darauf mit eigenen Aktionen darauf reagieren zu können.

6.3.2 Informationen an Beteiligte des Programms

Der Programmeigner wird ein stabil funktionierendes Informationssystem einrichten und betreiben, mit dem er interne Informationen an alle Beteiligten des Programms übermittelt. Dies kann z.B. ein monatlicher (oder bedarfsweiser) über das Internet an alle abonnierten Beteiligten sein, der über Neuerungen im Programm berichtet. Der interne Informationsdienst enthält keine vertraulichen Informationen. Er ist für die Nutzer kostenfrei.

6.3.3 Information und Beratung für Interessenten und Kunden

Der Programmeigner bietet für Interessenten und Kunden Information sowie Beratung gemäß Kapitel 3 dieses Handbuchs an. Er ist völlig frei in der Ausgestaltung dieser Aufgabe.

Der Programmeigner wird sich in generellen Fragen mit interessierten Zertifizierungsstellen, die Kundeninformationen zum Zertifizierungsprogramm bereitstellen (keine Beratung gemäß Kapitel 3 des Handbuchs), abstimmen, um hier gegenüber Interessenten und Kunden konzertiert aufzutreten.

6.3.4 Anerkennung der Zertifizierungsstellen

Der Programmeigner kann in einem formalisierten Anerkennungsverfahren interessierte zertifizierungsverfahren anerkennen für das Programm IWTS tätig zu sein.
Die Zertifizierungsstellen müssen hierzu einen formellen Antrag schriftlich an den Programmeigner stellen.

Im Antragsverfahren muss die Zertifizierungsstelle gegenüber dem Programmeigner nachweisen, dass sie die Anerkennungsvoraussetzungen (Kap. 6.2.1) erfüllt.

Erfüllt die antragstellende Zertifizierungsstelle die Voraussetzungen kann der Programmeigner die Anerkennung aussprechen. Im Anerkennungsschreiben kann er weitere programmbezogene Details festlegen, die die Zertifizierungsstelle bei der Anwendung seines Programms zu erfüllen hat. Nach dem Grundsatz der Transparenz und Neutralität sollen diese Details für alle Zertifizierungsstellen identisch sein. Ausnahmen erfordern eine schriftliche Begründung gegenüber dem Beirat.

Sowohl der Programmeigner als auch die Zertifizierungsstelle haben ein Kündigungsrecht.

6.3.5 Fortschreibung des Programms

Die Fortschreibung des Programms dient der Aufrechterhaltung, Verbesserung du Anpassung des Programms an innerhalb und außerhalb des Programms veränderte Rahmenbedingungen. Dazu sollte der Programmeigner ein Verfahren in Gang setzen, aus dem er regelmäßig Informationen aus der Gruppe der Beteiligten und der Gruppe der interessierten Kreise über die Akzeptanz des Programms und über Wünsche zu seiner Verbesserung entnehmen kann. Diese sind zu bewerten, um festzustellen was unverändert bleibt und was verbessert werden soll.

Die Analyse sollte sowohl die Programmanforderungen als auch die Zertifizierungsanforderungen umfassen (siehe ggf. unter Begriffe Kap. 3.).

a) Programmanforderungen: Hier ist kontinuierlich zu beobachten, die Gültigkeit und Vollständigkeit des FdWB-Standards (=Kriterien des kompletten Programms). Dabei ist insbesondere darauf

zu achten, ob bestimmte Normen und andere normative Dokumente verändert oder ungültig wurden, was Einfluss auf den FdWB-Standard hat.

b) Zertifizierungsanforderungen: Hier ist die Leitung und Lenkung des Programms insbes. der Programmanpassungen zu beobachte, sowie die Zufriedenheit der Zertifizierungsstellen, der Kunden und der interessierten Kreise.
c) Der Programmeigner überwacht, ob alle Zertifizierungsstellen ob sie nach den vom Programmhandbuch vorgeschriebenen Methoden und Verfahren gleichartig arbeiten, um so die Konsistenz der Ergebnisse aus dem Konformitätsbewertungsprozess aller Kunden sicherzustellen.

Die unter a) bis c) benannten Maßnahmen sind im 1. Schritt schriftlich als „Programmanpassung“ zu formulieren (Formularmuster als Anlage 1) und an alle Zertifizierungsstellen und Kunden zu übermitteln. Dabei sind die Programmanpassungen zu datieren und mit fortlaufender Nummer zu versehen, um allen Beteiligten Möglichkeit zu geben, die Vollständigkeit der Programmanpassungen selbst zu überwachen. Sie sind dann im zweiten Schritt zeitnah und in geeigneter Weise (z.B. Newsletter per Email) allen Beteiligten kostenlos zuzustellen.

6.3.6 Regelungen zur Transparenz

Der Programmeigner achtet darauf, dass er seine eigenen Maßnahmen mit höchster Transparenz vorbereitet und umsetzt, um die Zufriedenheit der Zertifizierungsstellen, Kunden und interessierten Kreise ständig zu sichern.

6.3.7 Öffentliches Verzeichnis aller Zertifikate

Der Programmeigner führt eine aktuelle Liste aller IWTS-Zertifikate und veröffentlicht diese im Internet. Dazu verpflichtet er im Anerkennungsverfahren (siehe Kapitel 6.3.4) die Zertifizierungsstellen, parallel mit der Zusendung des Zertifikats an den Webseitenbetreiber eine entsprechende Meldung auch an den Programmeigner zu geben.
An der gleichen Stelle, wo im Internet die gültigen Zertifikate veröffentlicht werden, werden auch bekannt gewordene Zertifikate folgender Kategorien veröffentlicht: ungültige, entzogene, gefälschte.

6.3.8 Kooperation mit anderen Zertifizierungsprogrammen oder -systemen

Sollten sich am Markt ähnliche Zertifizierungsprogramme oder -systeme für die Bewertung von Webseiten etablieren, *kann* der FdWB mit interessierten Programmeignern geeignete Kooperationen zum gegenseitigen Nutzen eingehen. Das kann die Vermeidung von Doppelzertifizierungen sein, bei der in jedem Zertifizierungsprogramm Elemente sind, die für die Nutzer jeweils einen hohen Wert haben, aber auch Elemente die sich doppeln. Das Gegenteil ist die kostengünstige Schließung von Lücken im eigenen Programm.
Beispiel: Gegenseitige Anerkennung von Zertifikaten für exakt definierte Kriteriengruppen. Hierdurch kann sich für den Zertifikatsnutzer die Aussagebreite seines Zertifikats erweitern ohne dass die Kosten proportional dazu steigen.
In jedem Fall muss dazu ein qualifiziertes Benchmarking durchgeführt werden, was auch den Ruf des anderen Programms und seines Eigners einschließen sollte.

7. Normative Verweise

a) Webseitensicherheit:

- Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- Verordnung über die Anforderungen an Vergleichswebsites nach dem Zahlungskontengesetz sowie an die Akkreditierung und Konformitätsbewertung (Vergleichswebsitesverordnung - VglWebV) vom 16. Juli 2018 (BGBl. I S. 1182)
- Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme – Anforderungen (DIN ISO/IEC 27001:2015-03)

Prüfbereich	**Kriterium**	**Kriterien-ID Dtl.**	**Kriterien-ID Int.**	**Quelle**
Cyber-Sicherheit	URL-Test	PP001	PE001	FdWB-Standard
	https:// URL	PP002	PE002	FdWB-Standard
	SSL/TLS – Secure Sockets Layer/Transport Layer Security Verschlüsselung	PP003	PE003	https://de.wikipedia.org/wiki/Transport_Layer_Security und https://de.wikibooks.org/wiki/IT-Sicherheit_f%C3%BCr_Privatanwender:_Grunds%C3%A4tze:_Transportverschl%C3%BCsselung
	Technischer Sicherheitstest	PP042	PE019	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
Datenschutz	HTTP-Cookie** vorhanden	PP004	-	https://www.gesetze-im-internet.de/tmg/__15.html und https://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html und http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=4667410 und Datenschutzrechtliche Pflichten der ePrivacy-Richtlinie 2002/58/EG („Cookie-Richtlinie“)
	Cookie-Hinweistext vorhanden?	PP005	-	https://www.gesetze-im-internet.de/tmg/__15.html und https://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html

Prüfbereich	Kriterium	Kriterien-ID Dtl.	Kriterien-ID Int.	Quelle
				und https://datenschutz-generator.de/eugh-urteil-like-button-cookie-opt-in-abmahnbarkeit/
	Möglichkeit, Cookies abzulehnen	PP006	-	https://www.gesetze-im-internet.de/tmg/__15.html und https://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html und https://datenschutz-generator.de/eugh-urteil-like-button-cookie-opt-in-abmahnbarkeit/
	Möglichkeit, Cookies zu erlauben	PP007	-	https://www.gesetze-im-internet.de/tmg/__15.html und https://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html und https://datenschutz-generator.de/eugh-urteil-like-button-cookie-opt-in-abmahnbarkeit/
	Link zur Datenschutzerklärung	PP008	-	https://www.bundestag.de/dokumente/textarchiv/2019/kw26-de-datenschutz-649218
	Link zur Datenschutzerklärung - zusätzliche Seiten in weiteren Sprachen	PP009	-	https://www.datenschutz.org/datenschutzerklaerung-mehrsprachig/
	Existiert eine Datenschutzerklärung?	PP010	-	https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html
	Existiert eine Datenschutzerklärung? - zusätzliche Seiten in weiteren Sprachen	PP011	-	FdWB-Standard
	Form der Datenschutzerklärung ist übersichtlich und gegliedert	PP012	-	FdWB-Standard

Prüfbereich	Kriterium	Kriterien-ID Dtl.	Kriterien-ID Int.	Quelle
	Form der Datenschutzerklärung ist übersichtlich und gegliedert - zusätzliche Seiten in weiteren Sprachen	PP013	-	FdWB-Standard
	Daten des Unternehmens in der Datenschutzerklärung	PP014	-	https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutz-grundverordnung.html
	Daten des Unternehmens in der Datenschutzerklärung - Seiten in weiteren Sprachen	PP015	-	FdWB-Standard
	Hinweispflicht Datenschutzbeauftragte/r	PP016	-	https://www.bundestag.de/dokumente/textarchiv/2019/kw26-de-datenschutz-649218
	Web-Kontaktformular/e: Datenschutzhinweis	PP017	-	https://www.e-recht24.de/dsgvo-gesetz.html und https://www.e-recht24.de/news/abmahnung/10651-abwarnung-kontaktformulare-einwilligung.html
	Web-Kontaktformular/e: Datenschutz Kontrollkästchen	PP018	-	https://www.e-recht24.de/dsgvo-gesetz.html und https://www.e-recht24.de/news/abmahnung/10651-abwarnung-kontaktformulare-einwilligung.html
	Web-Kontaktformular/e: Personenbezogene Datenerfassung	PP019	PE004	https://www.e-recht24.de/dsgvo-gesetz.html und https://www.e-recht24.de/news/abmahnung/10651-abwarnung-kontaktformulare-einwilligung.html
	Auskunftsrecht-Aufklärungspflicht (personalisierte Daten)	PP020	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO

Prüfbereich	Kriterium	Kriterien-ID Dtl.	Kriterien-ID Int.	Quelle
	Auskunftsrecht-Ablehnung (personalisierte Daten)	PP021	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
	Einwilligung in die Datenverarbeitung von Dritten (personalisierte Daten)	PP022	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
	Sichere Datenübertragung (im Internet)	PP023	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
	Kein pauschales Datensammeln (mit Formularen)	PP024	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
Inhaberschaft	Domain-Inhaberschaft bzw. Nutzungs-Berechtigung	PP025	PE005	https://www.denic.de/webwhois/
	Inhaberschaft Verifizierung Registerauszug	PP026	PE006	FdWB-Standard
	Inhaberschaft Verifizierung Gewerbeanmeldung	PP027	PE007	FdWB-Standard
	Inhaberschaft Verifizierung Rechnungsdokument	PP028	PE008	FdWB-Standard
	Impressum: Hinweis	PP029	PE009	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html
	Impressum: Weiterleitungs-Link zur Impressumsseite	PP030	PE010	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html

Prüfbereich	Kriterium	Kriterien-ID Dtl.	Kriterien-ID Int.	Quelle
	Impressum: Inhaberangaben/Unternehmensauskunft	PP031	PE011	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html
	Impressum: Sitz des Unternehmens	PP032	PE012	FdWB-Standard
	Impressum: Eingetragenes Unternehmen	PP033	PE013	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html
	Impressumangaben: Rechtsform des Unternehmens bei juristischer Person	PP034	PE014	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html
	Impressumsangaben: Kontaktmöglichkeit 1	PP035	PE015	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html
	Impressumsangaben: Kontaktmöglichkeit 2	PP036	PE016	FdWB-Standard
	Impressumsangaben: Vertretungsberechtigte bei juristischen Personen	PP037	PE017	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html
	Impressumsangaben: Registereintragung bei juristischen Personen	PP038	PE018	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html
	Impressumsangaben: Anerkennung bestimmter Berufsgruppen	PP039	-	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html

Prüfbereich	Kriterium	Kriterien-ID Dtl.	Kriterien-ID Int.	Quelle
	Impressumsangaben: Internetshops/Verkaufswebseiten	PP040	-	Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten und https://www.gesetze-im-internet.de/tmg/__5.html
Benutzerfreundlichkeit	Responsives Design: Erkennbarkeit des Inhalts bei mobilen Endgeräten	PP041	PE019	FdWB-Standard

b) Zertifizierungsmethodik

- ISO Guide 27:1983 Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity[1]
- DIN EN ISO/IEC 17000:2005-03 Konformitätsbewertung - Begriffe und allgemeine Grundlagen; Dreisprachige Fassung EN ISO/IEC 17000:2004
- ISO/IEC 17007:2009-09 Konformitätsbewertung - Leitlinien zur Erarbeitung von geeigneten normativen Dokumenten für die Konformitätsbewertung
- EN ISO/IEC 17030:2009 Konformitätsbewertung – Allgemeine Anforderungen an Konformitätszeichen einer dritten Seite (ISO/IEC 17030:2003) Deutsche und Englische Fassung EN ISO/IEC 17030:2009
- ISO/IEC 17065:2012-09 Konformitätsbewertung - Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren
- DIN EN ISO/IEC 17067:2013-12 Konformitätsbewertung - Grundlagen der Produktzertifizierung und Leitlinien für Produktzertifizierungsprogramme (ISO/IEC 17067:2013); Deutsche und Englische Fassung EN ISO/IEC 17067:201
- DIN EN ISO 19011:2018-10 Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018); Deutsche und Englische Fassung EN ISO 19011:2018

[1] "Dieser Standard wurde zuletzt im Jahr 2014 überprüft und bestätigt. Daher ist diese Version weiterhin aktuell. " Quelle (Juni 2019): https://www.iso.org/standard/19736.html

Anlagen

ANLAGE 1: FORMULARMUSTER „PROGRAMMANPASSUNG“

<table>
<tr><td colspan="3">Fachverband deutscher Webseiten-Betreiber GmbH (FdWB)</td></tr>
<tr><td colspan="3">Programm-Handbuch für die Zertifizierung von Webseiten nach dem IWTS-Programm</td></tr>
<tr><td>Programmversion:
Stand: Juni 2019;
Version: 0.0</td><td>Anpassung Nr.: XX/2019</td><td>Ausgabedatum: XX.XX. 2019</td></tr>
<tr><td>Betreff:
Kapitel XX,
Absatz XX, Nr. XX</td><td colspan="2">[welche Stelle im HB ist zu verändern?]</td></tr>
<tr><td>Änderungsgrund:</td><td colspan="2">[Beschreibung des Änderungsgrundes, z.B. Normenänderung oder Gesetzesänderung oder Lösung eines Prozesskonflikts; die geänderte Norm, das geänderte Gesetz, der Prozesskonflikt ist zu definieren]</td></tr>
<tr><td>Geänderter Text:</td><td colspan="2"></td></tr>
<tr><td>Gültig ab:</td><td colspan="2">[Es sollte eine ausreichende Zeitspanne zwischen Mitteilung der Programmanpassung an Zertifizierungsstellen und Zertifikatsnutzer gegeben sein, um die Umsetzung so vorzubereiten, dass Audits am Tag nach Geltungsbeginn fair und komplett ablaufen können.]</td></tr>
<tr><td>Anmerkungen:</td><td colspan="2"></td></tr>
</table>

ANLAGE 2: MUSTER FÜR DEN ANTRAG AUF ZERTIFIZIERUNG

Das Formblatt für den Zertifizierungsantrag gestaltet jede zertifizierungsstelle selbst in Anlehnung an die im Muster vorgegebenen Inhalte. Sie darf Hinzufügungen vornehmen.

<table>
<tr><td>[Name der Zertifizierungsstelle]</td><td>Programmhandbuch das Programm IWTS</td><td>Abschnitt XX
FM XX-XX</td></tr>
<tr><td>Datum: XX.XX.20XX</td><td>Version: 01</td><td>Seite: 52 von 56</td></tr>
<tr><td colspan="3">Antragsformular
für Inspektion und Zertifizierung nach dem Programm IWTS
durch die Zertifizierungsstelle [Name]…</td></tr>
<tr><td colspan="2">Name und Rechtsform des Antragstellenden Unternehmens:
(Bitte den vollen Unternehmensnamen eintragen.)</td><td>Adresse des Unternehmens:
(Straße, Hausnummer, PLZ, Stadt, Bundesland, Land, Postfach)</td></tr>
<tr><td colspan="2">Rechtlicher Vertreter des Unternehmens:
(Name und Funktion)</td><td>Kontaktperson für IWTS-Zertifizierung:
(Bitte ausfüllen, wenn nicht mit dem Rechtsvertreter identisch)</td></tr>
<tr><td colspan="2">Telefon:
Fax:
Mobil:</td><td>E-Mail:

Webseite:</td></tr>
<tr><td colspan="3">(Zutreffendes bitte ankreuzen)
☐ Erstmalige Antragstellung
☐ Änderungsanzeige (wenn Sie bereits Kunde der Zertifizierungsstelle sind)

Zutreffende Version des Programms IWTS bitte ankreuzen
☐
☐
☐
☐
☐
☐</td></tr>
<tr><td colspan="3">1. Information zum Unternehmen (Branche, Tätigkeit, Standorte)</td></tr>
</table>

4. Informationen zur Webseite, die zu Zertifizieren ist:
Domain:
Kurzbeschreibung:

5. Hat Ihr Unternehmen weitere Webseiten, die nicht zu zertifizieren sind (Ja/Nein)

4. Wurden Sie schon einmal durch eine andere Zertifizierungsstelle für das Programm IWTS registriert, auditiert oder zertifiziert?

Wenn ja, nennen Sie bitte: den Namen der Zertifizierungsstelle, das Jahr der Antragstellung, die frühere Registriernummer, die Gründe für den Wechsel.

6. Hier können sie noch weitere Angaben machen oder spezielle Wünsche äußern, die für die Zertifizierung Ihres Betriebes relevant sind, z.B. eine genauere detaillierte Beschreibung Ihrer Tätigkeit, die Reisezeit zwischen den verschiedenen Betriebsteilen (wenn zutreffend) usw.:

Der Unterzeichnende erklärt das Antragsformular wahrheitsgemäß und vollständig ausgefüllt zu haben

Name des Unternehmens: ……..

Rechtlicher Vertreter: ……..

Datum ……

Unterschrift: ……..

ANLAGE 3 AUDIT-ABLAUFBESCHREIBUNG

Direktzugang: IWTS-Audit-Portal
(für Auditoren und Zertifizierer): https://iwts-certificate.com/auditing-iwts/

1. Vorbereitung
    a. Initiale Aufforderung für das Audit ist die die Audit-Terminvorgabe.
    b. IWTS-Audit-Portal öffnen.
    c. Sichten, ob im IWTS-Portal Benachrichtigungen über neue Versionen, Hinweise oder Prüfanweisungen vorhanden sind.

2. Prüfung
   Prüfungsvoraussetzungen kontrollieren
    a. Login auf der Seite Auditing-IWTS mit persönlichem Auditoren-/Zertifizierer-Passwort.
    b. Sind die Kundendaten aus dem Antrag identisch mit den Daten im Prüfbereich (Name, Kundennummer, etc.) zu finden unter “Unternehmensdaten” im rechten Bildschirmbereich)?
    c. Sind Zuarbeiten vorhanden (erkennbar Status: Zuarbeiten vollständig. Sie finden alle Links unter “Zuarbeiten Dokumente”?

3. Audit/Zertifizierung
    a. Auf der rechten Seite sehen Sie alle Prüfpunkte. Bei Klick auf einen Prüfpunkt erscheinen die Varianten “konform” und “nicht konform” zum Abgleich.
    b. Tragen Sie in der Prüftabelle (linke Seite) Ihr Prüfergebnis mit evtl. Bemerkungen ein
    c. Im Feld "Ergebnis Audit" bzw. „Ergebnis Zertifizierung“ das Ergebnis des Audits/der Zertifizierung als Status festlegen. Der Status kann sein:
       “Auditing/Zertifizierung Warte-Status” oder “Audit/Zertifizierung ist vollständig abgeschlossen”.
       Ist eine Prüfung "nicht konform" oder gibt es offene oder ungeklärte Fragen, dann ist "Warte-Status" zu setzen.

4. Screenshots
   So erstellen Sie geeignete Screenshots
    a. Der Screenshot sollte immer den Prüfgegenstand und möglichst einen Bezug zur geprüften Webseite dokumentieren (Unternehmensname, -domain, -daten, -design).
    b. Speichern Sie die Screenshots bspw. in einem lokalen Bereich zwischen.
    c. Ändern Sie den Screenshot-Dateinamen:
       Kundennummer, Auftragsnummer, ID des Prüfpunkts, Anzahl Screenshot je Prüfpunkt, A oder Z (Auditor oder Zertifizierer), Datum.
       Beispiel: 123456-23450-3-1-A-11092019.jpg
    d. Nachdem alle Prüfpunkte ausgeführt wurden, bitte alle Screenshots im Feld “Upload der Screenshots-Au1” hochladen (Drag-and-drop).
    e. Achtung: Nach dem Hinzufügen der Dateien muss der Upload aktiv durch Klick auf den Button “Beginn Upload” gestartet werden!

5. Wo finde ich die Prüf-Tools:
   Audit-Seite rechts, unter dem Punkt “Prüf-Tools”.

6. Mit Klick auf “Absenden” wir die Prüfung abgeschlossen.
   Prüfen Sie bitte zuvor alle Eingaben.

7. Hinweise:
   Kontaktformular rechts: Hier können Sie Bemerkungen, Hinweise, Fehler o. ä. an die Technik senden.

   Wir haben das Ziel, dieses Portal so benutzerfreundlich wie möglich zu gestalten. Bitte unterstützen Sie uns dabei. Haben Sie Hinweise oder Fragen, dann schreiben Sie uns bitte eine Nachricht unter Kontakt/Kontaktformular.

ANLAGE 4: ÜBERSICHT ÜBER DIE PRÜF-TOOLS

Kriterium	Deutscher Standard	Internationaler Standard	Prüf-Tools	
	Kriterien-ID	Kriterien-ID	Name	Link
SSL/TLS	PP003	PE003	Comodo SSL Checker	https://comodosslstore.com/ssltools/ssl-checker.php
SSL/TLS	PP003	PE003	SSL Labs SSL Server Test	https://www.ssllabs.com/ssltest
Techn. Sicherheitstest	PP042	PE019	Sucuri Site Check	https://sitecheck.sucuri.net/
Cookies	PP004	-	Cookie-Metrix	https://www.cookie-metrix.com
Berechtigung URL-Nutzung	PP025	PE005	Qualidator DNS Report	https://www.qualidator.com/WQM/de/Tools/DNSReport.aspx
Unternehmenssitz	PP032	PE012	Deutsche Post	https://www.postdirekt.de/plzserver
Umsatzsteuer-ID	PP040	-	Umsatzsteuer-ID prüfen	https://ust-id-pruefen.de