Fachverband deutscher
Webseiten-Betreiber GmbH
- FdWB -

Program Manual
for the
Certification of Websites
with the program

"International Website Trust Standard" (IWTS)

Status: September 2024 Version: 5.2.1

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

Dr. habil. Rainer Friedel
Control Union Academy - The Sustainability Academy -
Dorotheastrasse 30, 10318 Berlin
Phone +49 (0)162 265 95 34
academy@controlunion.com
https://www.cu-academy.de/

Michael Turko
Fachverband deutscher Webseiten-Betreiber (FdWB)
Rahel-Hirsch-Straße 10, 10557 Berlin
Phone: +49 (0)30 4036 3580
fax: +49 (0)30 4036 35899
info@fdwb.de
https://fdwb.de

Content **Page**

1. The Fachverband deutscher Webseiten-Betreiber (FdWB) and the goals of its certification program

The Fachverband deutscher Webseiten-Betreiber (FdWB; Association of German Website Operators) supports users and end consumers of websites to recognize with a glance at the visited website whether the visited website is particularly secure and trustworthy. This significantly increases the frequency of use of the certified websites and the trust in their information. Website operators take measures to protect their websites with important standards and thus make an additional contribution to cyber security by protecting themselves and their visitors. These are decisive commercial advantages both for website operators and for the safety of website visitors and end users.

The technical background of the certification program is based on four quality-related principles:

a) The ***FdWB-Standard*** **"International Website Trust Standard (IWTS)"** contains a list of quality-relevant inspection criteria defined on the basis of recognized standards. They cover the areas of cyber security, data protection, ownership and identification obligations, and user-friendliness. The areas include the verification of confidence-building and security-relevant measures and information.
   The standard relieves both website operators and users of websites of the burden of knowing in detail about the necessary criteria of a quality-oriented website and of checking them with every visit, because the FdWB-Standard aggregates all this knowledge. Whoever follows the standard is on the safe side. Website operators and website users can rely on this. Websites marked with the IWTS conformity mark (logo) can be trusted.
b) The ***conformity inspections*** of the customer websites are carried out by certification bodies independent of the FdWB and the website operators. Their reliability and neutrality are ensured by accreditations, which must be completed annually.
c) The ***costs for certification*** are kept at a low level by using new, cost-saving inspection procedures for conformity inspection. This makes IWTS certification affordable even for website operators with a small budget. For customers of the IWTS certification program, the conformity mark is free of charge.
d) ***Advice*** for website operators who need support for the production of certifiable websites is provided by the FdWB and by website service providers cooperating with it.

The main objectives of the IWTS program are

- Website providers are enabled to advertise on the website market that their website has been reviewed by an impartial third party, with the result that it meets all requirements of the IWTS-Standard.
- The IWTS program is designed to help website users to distinguish between websites in terms of security and other usage criteria and to give preference to those that offer more security and service. Trust is created among website users who have an interest in secure websites.
- Provision of a commercial advantage for certified websites.

This manual sets out the criteria that website operators must comply with and all sub-processes of the certification procedure. It is binding for all parties involved in the certification process, especially certificate holders and certification bodies.

The FdWB will carefully monitor the timeliness of the criteria and the experience gained in the working process regarding the certification process, evaluate this at regular intervals with the advisory board and immediately implement program adjustments if a need is identified. These are transmitted in writing to the certification bodies and certificate users involved. In case of very substantial program adaptations or for the integration of a larger number of smaller program adaptations, a continued version of the IWTS program is created.

This manual has been compiled with the greatest care. If readers find gaps, the FdWB asks them to inform the FdWB of these observations.

No responsibility is taken for errors or mistakes. No warranty claims can be derived from this to the FdWB.

2. Purpose of this manual

The Program Manual for the IWTS Certification Scheme serves to describe the objectives and function of the program elements in order to create transparency for all parties involved for the similar application by all parties.

3. Definitions of terms

Recognised Certification Body means a certification body accredited by a national accreditation body and recognised by the IWTS program owner in accordance with the recognition procedure described in this Program Guide (Chapter 6.3.4).

Recognised auditor is a person who fulfils the technical and personnel requirements defined in this program manual and on the basis of this conformity is recognised by the certification body for his activities in the IWTS program. Only recognised auditors may be used for this activity (Chapter 6.2.1, points d) and e)).

Audit Inspection of the conformity of a website with the FdWB-Standard by a recognized auditor from a recognized certification body. Audits can be conducted as on-site audits and desk audits. They are based on the regulations of ISO 19001.

The Advisory Board is a body that supports the real functioning of the IWTS program. The advisory board advises the management of the FdWB. It also acts as a conciliation committee in the event of objections from certification bodies or from customers if the facts of the case exceed the responsibility of the certification body. It should be representative of the 'interested parties' and should not exceed 5 persons.

Benchmarking is a systematic and documented comparison of the performance of different certification programs, usually with the aim of checking or realizing a cooperation between the programs. This is usually aimed at economic advantages for program owners, certification authorities and certificate users (Chapter 6.3.8).

Consulting in this context is the activity of providing support to a website operator, planning, developing, operating or marketing websites. Certification bodies are not permitted to engage in this activity in order to avoid conflicts of interest in their certification decision.
For the FdWB the prohibition of consulting does not apply.

Participants of the IWTS program are: the program owner Fachverband deutscher Webseiten-Betreiber GmbH (FdWB) and its organs, all recognised certification bodies and all certificate holders (= website operators).

FdWB-Standard is a description of all website properties (= requirements for the website) of the website operators that are necessary to achieve the goals of the FdWB certification program (chapter 5.4).

An ***interested party*** is a website operator who is interested in certification against the FdWB-Standard but has not yet submitted an application to a certification body.

Stakeholders are natural or legal persons and other groups that participate in or feel affected by the IWTS program (e.g. website operators, website users, certification bodies, customers, authorities, etc.).

Conformity with all requirements described in the FdWB-Standard is a prerequisite for the issue of a certificate. It must be ensured that the product requirements and the certification requirements are equally fully met.

Users of websites are legal or natural persons, especially end users who use websites. They are usually not experts on the functionality and security of websites. But they are interested in knowing

if the visited website is secure and trustworthy. The IWTS logo provides the desired positive information at a glance and thus creates commercially beneficial trust for the website operator.

Product requirements are the criteria for all features of the website, which are defined in the FdWB-Standard (chapter 5.4) The criteria are (usually) specified by third party standards. Compliance with all criteria must be completely inspected in the certification process during the audit.

Program adaptation is a measure taken by the program owner to identify and implement[1] selective changes in the program and to communicate them to the certification authorities and certificate users. The form (Annex 1) is used for this purpose. The starting point for program adjustments can be: normative or legal changes to the criteria described in chapter 5.4 of this manual. Insights into improving processes defined in the program manual can also lead to program adjustments. The need for program adjustments must be monitored, identified and formulated by the program owner. Intended program adjustments are to be submitted to the Advisory Board for decision.

If there is a need for general changes to the program, e.g. because a large number of program adaptations have been made in the meantime, the program owner creates a new version of the program (see chapter 6.3.5 of this manual). The program owner may call on external experts for this purpose. The new version is to be submitted to the Advisory Board for approval.

Program owner (program sponsor) is an individual or organization responsible for developing and maintaining a specific certification program (ISO 17067). Program owner of the IWTS program is the FdWB.

Inspection mark (conformity mark, certification mark, logo) The IWTS inspection mark is a registered word and image mark and is the conformity mark of the IWTS program. It informs the user of a website at a glance that this website has been checked against the FdWB-Standard by means of the IWTS program and therefore has special security features. The mark is property of the program owner. It can be used free of charge by all participants in the IWTS program to mark the website itself and documents related to the IWTS program as eye-catchers (details in chapter 6.1.5).

Quality level The IWTS program can have different variants, globally or by region and country (International, German-DE, USA-USA, China-CHN, Austria-AUT, Switzerland-CHE and others). Details must be presented in writing by updating the program.

The *risk of* a website is defined in this certification program depending on the compliance with legal regulations in the areas of cyber security, DSGVO (German Data Protection Act), identification requirements according to the applicable Telemedia Act and EU regulations as well as additional extensive protective measures defined in the IWTS standard.

The inspection points of the IWTS standard define the condition.

Website operators are commercial, freelance or legal persons (no natural persons in the sense of an end user - these are website owners), who provide information to certain target groups with the help of a website. As a rule, they have no expert knowledge about the security and technical quality of a website and have to have this done by service providers without being able to assess the quality of the service themselves. The application of a quality and security standard whose conformity with the standard is certified gives the website operator confidence in his own website and commercial advantages, if the users of his website can also gain confidence in the website by looking at the IWTS logo.

According to ISO 17065, ***customer*** is the organization or person responsible to a certification body for ensuring that the certification requirements, including product requirements, are met. Under this certification program, the customer is a commercial, freelance or legal entity (not a natural person in the sense of an end user) who is responsible for fulfilling the legal requirements for the security and quality of the website and, as an authorized signatory, signs the certification contract with the certification authority.

[1] The program owner may call on external experts for this purpose.

Other definitions in certain legal regulations, e.g. HGB, German Civil Code (§ 312c), Telemedia Act (§ 5), DSGVO or others, are not applicable in this narrowly defined context, if the regulation is not contradictory to the legal regulations.
All certified website operators are published on the Internet by the program owner (details in chapter 6.3.7 of this manual).

Certificate is the document which, based on the inspection of a website with a defined procedure by an accredited and FdWB-approved certification body, confirms that this website fully meets all criteria of the FdWB-Standard, which is part of this program manual. The certificate is the property of the issuing certification body. The latter is the basis for the fact that the certification body can withdraw the certificate at any time if the certificate user does not ensure the conformity of his website with the FdWB-Standard within a reasonable period of time.

Certificate users are commercial, freelance or legal persons (no natural persons in the sense of an end user) who use a certificate issued by a competent certification body for their purposes on the basis of a valid certification agreement.

Certification requirements are the common set of product requirements plus the requirements that the certification process places on the customer. The requirements for the certification procedure are in turn the common requirements that the certification program plus the certification body impose on the customer. For a successful certification decision, all certification requirements must be fully examined and fulfilled.

Certification scheme is a system, usually set out in writing, that describes the requirements (= criteria), rules and procedures to certify certain products, processes and services. Program owners should, when developing certification programs, in addition to the requirements to be met by the users (customers), also meet the formal requirements of ISO 17067. Certification bodies certifying products, processes and services should be accredited to ISO 17065. Companies wishing to have their products, processes or services certified should thoroughly prepare both the selection of the certification program that best suits their needs and the fulfilment of all requirements of the certification program before the first audit.

4. Entry into force

The Program Manual for the certification of websites according to the IWTS program will come into force as version 1.1 with its publication on 21.09.2020.

It is binding for all participants in the IWTS program.

5 The IWTS certification program

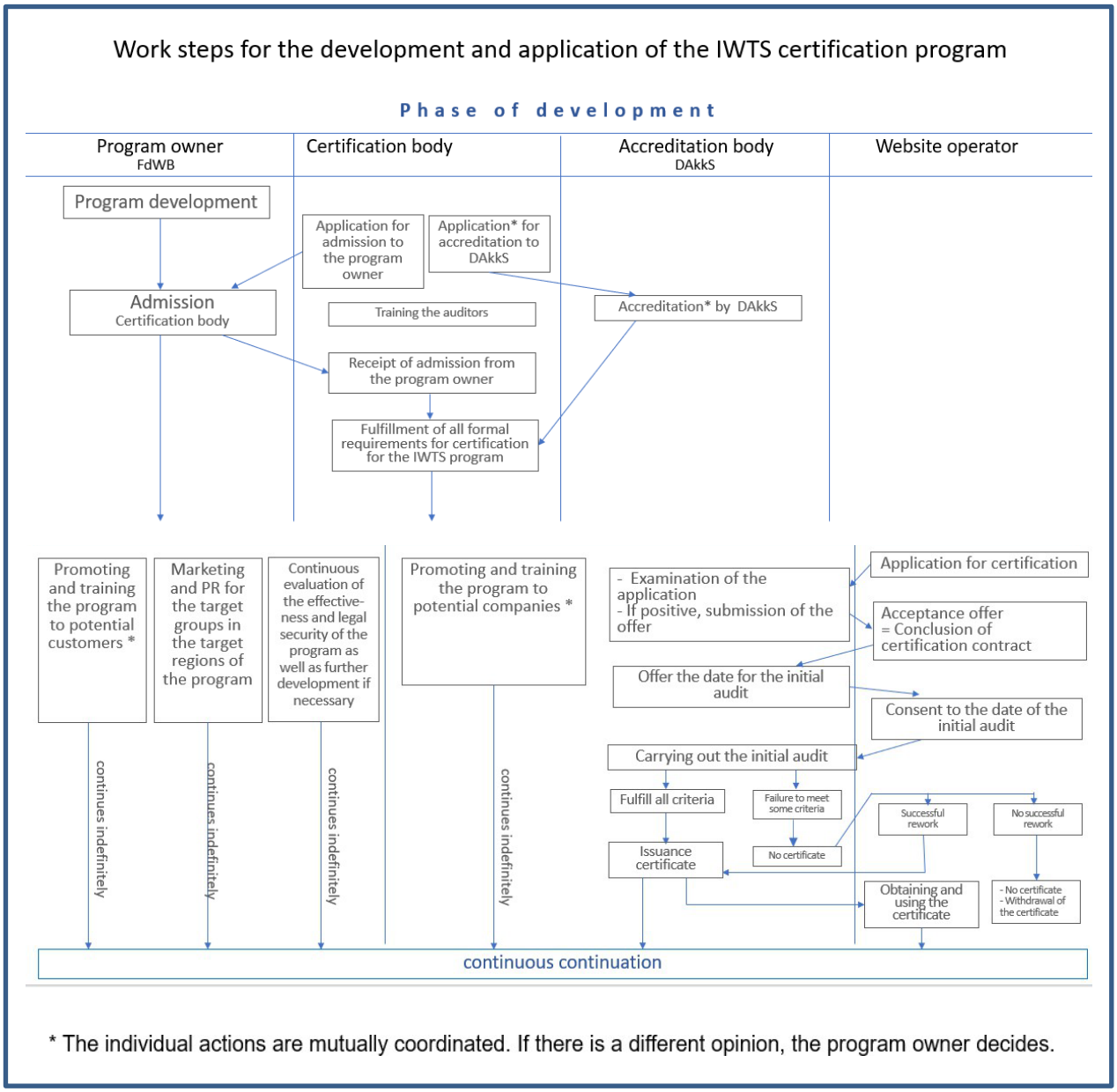
5.1 Application area

This manual describes the objectives, subject matter and function of the IWTS Program Certification Scheme. This program is to be used to organize the cooperation of program owners, certification bodies and website operators in such a way that it is much easier for website operators, who are usually not experts in the security and technical functioning of websites, to find secure and well-functioning websites with little effort.

Using ISO 17067, the program has been designed in such a way that the certification process is carried out by a neutral third party by certification bodies that perform their work on the basis of ISO 17065.

5.2 Structure and function of the certification scheme

Figure 1 shows the development, structure and application of the IWTS program.



5.3 Trial phase

Upon completion of the program development, the program owner will appoint a suitable certification body to test the program for up to 2 years. The trial period is intended to allow the company to gain experience with the application of the program and to be able to make rapid improvements to the program while still having a manageable number of customers.

The detailed inspection program will be developed jointly by the FdWB and the selected certification body at the appropriate time and then applied in practice in certification.

5.4 The FdWB-Standard for safety and quality

5.4.1 IWTS-Standard version German

Inspection area	**Criterion**	**Extended notes for criterion**	**criteria number**	**Criteria ID**	**conform**	**non-conform[1]**
Cyber Security	URL test	No open redirection to other URL after calling the operator web page URL	1	PP001	The URL specified in the application does not change when it is called up in the browser (no forwarding).	The URL specified in the application for certification changes after it is called up in a browser (redirection).
	https:// URL	Hypertext Transfer Protocol Secure (HTTPS)	2	PP002	The URL called up in the browser first shows these 8 characters, starting from the beginning: https://[2] The result is to be documented by a screenshot (see program manual appendix 3 point 4).	The 8 characters https:// are not displayed first from the front or are not clear.
	SSL/TLS - Secure Sockets Layer/Transport Layer Security Encryption	Functional test SSL/TLS certificate Communication protocol Transport Layer Security, strong encryption of the communication protocol	3	PP003	The SSL/TLS certificate is tested with the Comodo SSL Checker tool (https://comodosslstore.com/ssltools/ssl-checker.php) and the SSL Labs SSL Server Test tool (https://www.ssllabs.com/ssltest) and the result contains no security or warning messages (all results are green). The result of the inspection of this point has a direct effect on PP023. Both inspection points always directly assume the same state.	The SSL/TLS certificate is tested with the Comodo SSL Checker tool and the SSL Labs SSL Server Test tool and the result shows at least one security or warning message (marked red/orange). The result of the inspection of this point has a direct effect on PP023. Both inspection points always directly assume the same state.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					The result is to be documented by a screenshot (see program manual appendix 3 point 4).	
	Technical safety test	Checking the website for currently known and relevant malicious systems, malware and security holes (including malware, viruses, official blacklists)	4	PP042	Checking the website with the "Sucuri Site Check" tool (https://sitecheck.sucuri.net/) produces an overall result of only a "minimal" or at most "low" risk and is therefore green in each case. The result is to be documented by a screenshot (see program manual appendix 3 point 4).	Checking the website with the "Sucuri Site Check" tool gives an overall result higher than "low risk" and is therefore orange or red.
Data protection[3]	[4]HTTP cookie and cookie hint banner	Checks if cookies are present and cookie hint banner is needed	5	PP004	Either a): A fixed pop-up window or a similar display with a cookie hint banner will be shown at the latest after the website has been loaded. The check with the cookie test tool "CookieMetrix" (https://www.cookiemetrix.com/) shows that cookies of the green line or other cookies (orange, red line) are present. Or b): There is no fixed pop-up window or similar display with a cookie hint banner and the test with the cookie test tool "Cookie-Metrix" shows that only cookies of the green line (technical cookies) are visible.	A cookie hint banner is not available and the check with the cookie test tool "CookieMetrix" shows that besides technical cookies (green line) there are other cookies (in orange, red line).

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					If result a) is obtained, inspection points PP005 to PP007 shall be inpsected subsequently. For result b), inspection points PP005 to PP007 are not relevant. The result is to be documented by a screenshot (see program manual appendix 3 point 4).	
	Cookie hint text available?	Optional inspection point	6	PP005	This inspection point is relevant if PP004 was inspected for conformity on the basis of subpoint a): Necessary contents of the banner text are the information that the website uses cookies, a reference to the right of objection and to data protection, with a link to the website's privacy policy. The data protection declaration opens when you click on the link in the same or a new tab, a new page or as a banner element (popup or similar) ("data protection" and "data protection declaration" are permissible as designations). The result of the inspection of this point has a direct effect on PP020. Both inspection points always directly assume the same state.	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a): If the content of the banner text does not contain the necessary information such as right of objection or data protection or the link to the data protection declaration does not work or is not correctly identified. The result of the inspection of this point has a direct effect on PP020. Both inspection points always directly assume the same state.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
	Ability to refuse cookies	Optional inspection point	7	PP006	This inspection point is relevant if PP004 was inspected for conformity on the basis of subpoint a): An opt-out button[5] with the clear text "do not use cookies" (or similar) or a clear link to the corresponding place on the website where the cookie use can be rejected by clicking on it must be present in the cookie notice if cookie use is intended. The result of the inspection on this point has a direct effect on PP021. Both inspection points always directly assume the same state.	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a): If there is no opt-out button or no clear link to the appropriate place on the website where cookie use can be rejected by clicking on it, or if the content of the "do not use cookies" notice text (understood or similar) is not present either in the cookie notice or on the linked page. The result of the inspection on this point has a direct effect on PP021. Both inspection points always directly assume the same state.
	Possibility to allow cookies	Optional inspection point	8	PP007	This inspection point is relevant if PP004 was inspected for conformity on the basis of subpoint a): There must be an opt-in button[6] or link that must be clicked for active consent to the use of cookies by clicking, with the clear text "use/allow cookies" (or similar). The result of the inspection of this point has a direct effect on PP022. Both inspection points always directly assume the same state.	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a): There is no opt-in button or link that must be actively clicked to use cookies or that does not contain the unique "use/allow cookies" (or similar) notice. The result of the inspection of this item has a direct effect on PP022. Both inspection points always directly assume the same state.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
	Link to privacy policy	Inspection of removal requirements	9	PP008	On any web page of the domain to be checked, in the header (top) or footer (bottom), clearly visible, a link with the designation "Privacy Policy" or "Privacy" is displayed, which links to the Privacy Policy. The result from one side is to be documented by a screenshot (see program manual appendix 3 point 4).	It is not displayed on any website of the domain to be checked in the header (top) or footer (bottom), clearly visible a link labeled "Privacy Policy" or "Privacy" or the link does not link to the Privacy Policy.
	Link to privacy policy - additional pages in other languages	Optional inspection point Inspection of removal requirements	10	PP009	If the website is additionally offered in English or another language, a translation of the privacy policy must be available in the respective language and the same verification criteria apply as for the German language part: In the header (top) or footer (bottom) of any web page of the domain under review, a clearly visible link with the designation "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" or "Data Protection Declaration" or, in the case of an additional English language version, with the designation "Privacy Policy" or "Data Protection" (or similar designation) in the relevant language, will be displayed on any web page of the domain	If the website is additionally offered in English or another language, a translation of the privacy policy must be available in the respective language and the same verification criteria apply as for the German language part: In the case of an additional English language version, a link with the designation "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" or "Data Protection Declaration" or, in the case of an additional language version, with the designation "Privacy Policy" or "Data Protection" (or similar designation) in the relevant language will not be displayed in the header (top) or footer (bottom) of any website of the domain to be checked, or the link will not link to

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					under review, linking to the relevant language version of the Privacy Policy. The result from one side is to be documented by a screenshot (see program manual appendix 3 point 4).	the Privacy Policy in the relevant language version.
	Is there a privacy policy?	Inspection of removal requirements	11	PP010	By clicking on a link or menu item "Privacy Policy" you will be redirected to an extra page with the heading "Privacy Policy". On this page there is an easily recognizable text that deals with the topic of data protection. The result is to be documented by a screenshot (see program manual appendix 3 point 4).	It is not possible to find a link or a menu item with the name "Privacy Policy" or on the target page there is no heading "Privacy Policy" or no text content on the subject of privacy.
	Is there a privacy policy? - additional pages in other languages	Optional inspection point Inspection of removal requirements	12	PP011	If the website is additionally offered in English or another language, a translation of the privacy policy must be available in the respective language and the same verification criteria apply as for the German language part: By clicking on a link or menu item "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" or "Data Protection Declaration", in the case of an English language version, or in the case of another language with the designation "Privacy	If the website is additionally offered in English or another language, a translation of the privacy policy must be available in the respective language and the same verification criteria apply as for the German language part: It is not possible, in the case of an English language version, to create a link or menu labelled "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" or "Data Protection Declaration" or, in the case of another language,

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					Policy" or "Data Protection" (or If you click on "Privacy Policy" in the relevant language, you will be redirected to a separate page which, in the case of an English language version, has the heading "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" or "Data Protection Declaration" or, in the case of another language, the heading "Privacy Statement" or "Data Protection" (or similar term) in the relevant language. On this page you will find an easily recognizable text that deals with the topic of data protection in the respective language. The result is to be documented by a screenshot (see program manual appendix 3 point 4).	labelled "Privacy Policy" or "Data Protection" (or similar term) in the language concerned or, in the case of an English language version, there is no heading "Privacy Policy", "Data Privacy Statement", "Data Privacy Information" or "Data Protection Declaration" or, in the case of another language, no heading "Privacy Policy" or "Data Protection" (or similar term) in the language concerned or no text content on the subject of data protection in the language concerned.
	Form of the privacy policy is clear and structured	Inspection of removal requirements	13	PP012	The privacy policy is provided with headings, topic blocks, structured bullets and paragraphs.	The data protection declaration consists only of continuous text or has no structured character.
	Form of the privacy policy is clear and structured - additional pages in other languages	Optional inspection point Inspection of removal requirements	14	PP013	If the website is additionally offered in English or another language, a translation of the privacy policy must be available in the respective language and the same verification criteria apply as for the German language part:	If the website is additionally offered in English or another language, a translation of the privacy policy must be available in the respective language and the same verification criteria apply as for the German language part:

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					The privacy policy in the respective language is provided with headings, topic blocks, structured bullet points and paragraphs.	The data protection declaration in the respective language consists only of continuous text or has no structured character.
	Data of the company in the privacy policy	Inspection of removal requirements	15	PP014	Under one of the headings on the privacy statement page, the company name, address and contact details are easily identifiable[7]. The result is to be documented by a screenshot (see program manual appendix 3 point 4).	There are no or no complete details of the company name, address and contact details.
	Company data in the privacy policy - pages in other languages	Optional inspection point Inspection of removal requirements	16	PP015	If the website is additionally offered in English or another language, a translation of the privacy policy must be available in the respective language and the same verification criteria apply as for the German language part: Under one of the headings on the privacy statement page, the company name, address and contact details are easily identifiable. The result is to be documented by a screenshot (see program manual appendix 3 point 4).	If the website is additionally offered in English or another language, a translation of the privacy policy must be available in the respective language and the same verification criteria apply as for the German language part: There are no or no complete details of the company name, address and contact details.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
	Duty to inform data protection officers	Optional inspection point Inspection of removal requirements	17	PP016	This inspection point is only relevant if the applicant's answer in the prepayment form shows that a data protection officer is needed in the company. Otherwise this inspection point is omitted: A data protection officer must be appointed with name and contact details on the privacy statement page. The result is to be documented by a screenshot (see program manual appendix 3 point 4).	If, according to the information provided by the applicant in the preparatory form, a data protection officer must be appointed in the company, but no data protection officer is identified on the data protection declaration page.
	[8]Web contact form/s : Privacy policy	Inspection of removal requirements	18	PP017	Any contact/newsletter form or other data collection form must visibly indicate the privacy policy of the website, with the word "privacy" or "privacy statement", above the "submit" button (or similar term) and be associated with "consent". For this inspection, all pages[9] of the website to be certified must be searched for forms. Result of the complete form is to be documented by screenshot (program manual Appendix 3 point 4).	In at least one form offered on the site, the visible privacy notice of the website above the "Send" button (or similar term), marked with the word "Privacy" or "Privacy Policy" and associated with "Consent" is missing. For this inspection, all pages of the website to be certified must be searched for forms.
	Web contact form(s): Privacy checkbox	Checkbox not filled	19	PP018	If the contact form is designated as a newsletter or for notification actions which enable any unsolicited sending of	If the contact form is designated as a newsletter or for notification campaigns, which enables any unsolicited sending of

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					data to the sender of the data, an unfilled checkbox must exist for the data protection notice, which must be activated before the form data can be sent in order to confirm consent to the data protection notice. For this inspection, all pages of the website to be certified must be searched for forms. Result of the complete form is to be documented by screenshot (program manual Appendix 3 point 4).	data to the sender of the data, there is no unfilled checkbox for the data protection notice, which must be activated before the form data can be sent in order to consent to the data protection notice. For this inspection, all pages of the website to be certified must be searched for forms.
	Web contact form/s: Personal data collection	No blanket data collection, no blanket mandatory fields	20	PP019	Only necessary data such as salutation, name, e-mail address, subject and text message are requested in a contact form through defined mandatory fields. All other requested data must not be mandatory fields. If it is a newsletter subscription, only the e-mail field may be a mandatory field. For this inspection, all pages of the website to be certified must be searched for forms. The result of the inspection of this point has a direct effect on PP024. Both	In a contact form, in addition to the data or questions such as salutation, name, e-mail address, subject, text message or, in the case of a newsletter registration, in addition to the e-mail field, further data are requested which are marked as mandatory fields or without whose entry the sending of the form/registration is technically prevented. For this inspection, all pages of the website to be certified must be searched for forms.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					inspection points always directly assume the same state.	The result of the inspection of this point has a direct effect on PP024. Both inspection points always directly assume the same state.
	Right of access to information (personalised data)	Inspection Data Protection DSGVO/TMG	21	PP020	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a): Necessary contents of the banner text are the information that the website uses cookies, a reference to the right of objection and to data protection, with a link to the website's privacy policy. The data protection declaration opens when you click on the link in the same or a new tab, a new page or as a banner element (pop-up or similar) ("data protection" and "data protection declaration" are permissible as designations). The inspection procedure for this inspection point corresponds to PP005. Both inspection points always directly assume the same state.	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a): If the content of the banner text does not contain the necessary information such as right of objection or data protection or the link to the data protection declaration does not work or is not correctly identified. The inspection procedure for this inspection point corresponds to PP005. Both inspection points always directly assume the same state.
	Right of access refusal (personalised data)	Inspection Data Protection DSGVO/TMG	22	PP021	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a):	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a):

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					An opt-out button with the clear text "do not use cookies" (or similar) or a clear link to the corresponding place on the website where the cookie use can be rejected by clicking on it must be present in the cookie notice if cookie use is intended. The inspection procedure for this inspection point corresponds to PP006. Both inspection points always directly assume the same state.	If there is no opt-out button or no clear link to the appropriate place on the website where cookie use can be rejected by clicking on it, or if the content of the "do not use cookies" notice text (understood or similar) is not present either in the cookie notice or on the linked page. The inspection procedure for this inspection point corresponds to PP006. Both inspection points always directly assume the same state.
	Consent to data processing by third parties (personalised data)	Inspection Data Protection DSGVO/TMG	23	PP022	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a): There must be an opt-in button or link that must be clicked for active consent to the use of cookies by clicking, with the clear text "use/allow cookies" (or similar). The inspection procedure for this inspection point is the same as PP007. Both inspection points always directly assume the same state.	This inspection point is relevant if PP004 has been inspected for conformity on the basis of sub-item a): There is no opt-in button or link that must be actively clicked to use cookies or that does not contain the unique text "use/allow cookies" (or similar). The inspection procedure for this inspection point is the same as PP007. Both inspection points always directly assume the same state.
	Secure data transmission (on the Internet)	Inspection Data Protection DSGVO/TMG	24	PP023	The SSL/TLS certificate is tested with the Comodo SSL Checker tool (https://comodosslstore.com/ssltools/ssl-checker.php/) and the SSL Labs SSL Server Test tool	The SSL/TLS certificate is tested with the Comodo SSL Checker tool and the SSL Labs SSL Server Test tool and the result shows at least one security or truth

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					(https://www.ssllabs.com/ssltest/) and the result contains no security or warning messages (all results are green). The inspection procedure for this inspection point corresponds to PP003. Both inspection points always directly assume the same state.	indicator (marked red/orange). The inspection procedure for this inspection point corresponds to PP003. Both inspection points always directly assume the same state.
	No blanket data collection (with forms)	Inspection Data Protection DSGVO/TMG	25	PP024	Only necessary data such as salutation, name, e-mail address, subject and text message are requested in a contact form through defined mandatory fields. All other requested data must not be mandatory fields. If it is a newsletter subscription, only the e-mail field may be a mandatory field. The inspection procedure for this inspection point corresponds to PP019. Both inspection points always directly assume the same state.	In a contact form, in addition to the data or questions such as salutation, name, e-mail address, subject, text message or, in the case of a newsletter registration, in addition to the e-mail field, further data are requested which are marked as mandatory fields or without whose entry the sending of the form/registration is technically prevented. The inspection procedure for this inspection point is the same as PP019. Both inspection points always directly assume the same state.
Ownership	Domain ownership or right of use	Authorization URL usage	26	PP025	The Customer has confirmed in the assignment form that he has deposited the key for the domain holder verification and the Customer has deposited the key shown to him in the order protocol in the form "iwts-site-verification-[Key]" in the DNS report of his domain or server host	The customer has not stored a key or a key that differs from the order protocol in the DNS report of his domain or server host.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					and the verification with the tool Qualidator DNS Report (https://www.qualidator.com/WQM/de/Tools/DNSReport.aspx) confirms that the key has been deposited. The result of the inspection result with the DNS Report Tool must be documented by means of a screenshot (see program manual Appendix 3, point 4).	
	Ownership Verification Register extract	Optional inspection point Preliminary documentsError	27	PP026	Either the applicant has indicated in the application that he is subject to the obligation to register and has sent a document "extract from the register" in advance. Then check whether the company, owner, address and registration data of the document correspond with the data on the website to be certified. Or the applicant has indicated in the application that he is not required to be registered.	Either the applicant has indicated in the application that he/she is subject to the obligation to register but has not sent an "extract from the register" document in advance. Or the applicant has indicated in the application that he is subject to the obligation to register and has sent a document "extract from the register" in advance. However, the company, owner, address or registration data in the document do not match the data on the website to be certified.
	Ownership Verification Business registration	Optional inspection point Preliminary documentsError	28	PP027	This inspection point is only relevant if the applicant has indicated in inspection point PP026 that he is not subject to registration: Either the applicant has indicated in the application that he/she is obliged to	This inspection point is only relevant if the applicant has indicated in inspection point PP026 that he is not subject to registration: Either the applicant has stated in the application that he is obliged to register a

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					register a trade and has sent a "trade registration" document in advance. Then check whether the company, owner, address and registration data of the document correspond with the data on the website to be certified. Or the applicant has stated in the application that he is not required to register a business.	trade but has not sent a document "Trade Registration" in advance. Or the applicant has indicated in the application that he/she is obliged to register a trade and has sent a document "Trade Registration" in advance. However, the company, owner, address or registration data in the document do not match the data on the website to be certified.
	Ownership Verification Invoice document	Optional inspection point Preliminary documentsError	29	PP028	This inspection point is only relevant if there is no other document corresponding to inspection points PP026 or PP027: It is necessary to check whether a document "invoice document" (consumption, rental, electricity or Internet connection bill) has been sent in advance and whether the company, owner and address details match the details on the website.	This inspection point is only relevant if there is no other document corresponding to inspection points PP026 or PP027: No "invoice document" (consumption, rental, electricity or Internet connection bill) has been sent by the applicant in advance or the company, owner or address data in the document do not match the data on the website to be certified.
	Imprint: Note	Unambiguous possibility of perception	30	PP029	On any web page of the domain to be checked, in the header (top) or footer (bottom), a link with the name "Imprint" is clearly visible, which links to the imprint page. Alternatively, the complete imprint information can be displayed clearly visible on each page instead, as required in inspection points PP031 to PP040.	A link with the designation "Imprint" or the complete imprint information, as required in check points PP031 to PP040, is not displayed clearly visible on any web page of the domain to be checked, in the header (top) or footer (bottom).

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					The result of a page is to be documented by a screenshot (see program manual appendix 3 point 4).	
	Imprint: Forwarding link to the imprint page	Link to imprint page available	31	PP030	When clicking also the link "Imprint", a new area or a new page with the designation Imprint and the imprint content must be visible. Result of the complete imprint is to be documented by screenshot (program manual appendix 3 point 4 to be observed).	If you also click on the link "Imprint" the imprint data is not visible.
	Imprint: Owner data/company information	Mandatory data Owner data	32	PP031	The information on company name, owner first and last name, address (street, house number, postcode, city) is available.	One or more mandatory details of the company are missing, such as: Company name, first and last name of the owner, address (street, number, postcode, city).
	Imprint: Seat of the company		33	PP032	The owner business location must be in Germany and thus have a German address as imprint information. The German address must be the business address and must appear at the top as the first address if there are several branches within or outside Germany. For verification purposes, it must be checked that the postal code can be assigned to the Federal Republic of Germany (BRD). The unambiguous check is	The address given at the top of the imprint is not a German location. The specified postal code does not exist or is not located in the FRG.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
					performed with the tool https://www.postdirekt.de/plzserver/.	
	Imprint: Registered company	Optional inspection point Verification whether the entity is a legal person	34	PP033	This inspection point is only relevant if the company of the website to be checked is a registered company, but not for individual companies: The applicant's indication in the certification application whether the applicant is a registered legal entity was answered with "Yes" and an extract from the register, which the applicant has submitted, is available as a document copy.	This inspection point is only relevant if the company of the website to be checked is a registered company, but not for individual companies: The applicant has stated in the application that the company is a registered company (as a legal entity), but no excerpt from the register is available as a document copy, or the applicant has stated in the application that the company is not a registered company (as a legal entity), but the form of company stated in the imprint indicates that it is a registered company (as a legal entity).
	Imprint details: Legal form of the company in the case of a legal entity	Optional inspection point	35	PP034	In the case of legal entities, the company legal form must be[10] written out in full or as an abbreviation after the company name.	The company is a legal entity, but the legal form is neither abbreviated nor written out in full after the company name.
	Imprint details: Contact possibility 1		36	PP035	One of the following contact options must be available: e-mail address, telephone number, fax number, contact form.	None of the following contact details are given: E-mail address, telephone number, fax number, contact form.
	Imprint details: Contact possibility 2		37	PP036	There must be another contact possibility (unequal to contact possibility 1): e-mail address, telephone number, fax number, contact form.	Only one or none of the contact details is given.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
	Imprint details: Authorized representatives for legal persons	Optional inspection point	38	PP037	Indication of the first name and surname of the authorised representative.	The name of the authorised representative has been given incompletely or not at all.
	Imprint details: Registration of legal entities	Optional inspection point	39	PP038	Indication of the registration number of the trade/association/partnership or cooperative register and the name and seat of the competent district court.	One, several or all details of the registration number or name or seat of the competent district court are missing.
	Imprint details: Recognition of certain professions	Optional inspection point	40	PP039	Mandatory information for certain professions and situations provided by the applicant in the application or assignment form: a) The legal professional title and the State in which it was conferred. b) The name of the professional regulations and how to access them. (c) contact details of the chamber, authority or appeal body.	One, more or all of the information in (a), (b) or (c) is missing, even though the applicant has provided information on this in the pre-work form.
	Imprint details: Internet shops/selling websites	Optional inspection point Indication of the international sales tax ID	41	PP040	Specification of the international sales tax ID for webshops and sales pages[11], consisting of a fiscal identification number, the international country code ”DE” and a nine-digit number sequence. Using the tool "Check VAT ID" (https://ust-id-pruefen.de/), it is successfully checked that the VAT ID is valid and from Germany.	The international VAT ID was not or not completely specified or the check using the tool "Check VAT ID" (https://ust-id-pruefen.de/) shows that the VAT ID is not valid or not from Germany.

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
User-friendliness	Responsive design: Recognizability of content on mobile devices	Mobile Version Responsive Test	42	PP041	The presence of the view in the Responsive Design is checked with Google's Chrome browser. To do this, switch to the mobile, responsive view in the developer tools in the Chrome browser (Menu -> More tools -> Developer tools) and select a display width of 320 pixels (upper bar; view "Mobile S"). In the mobile view, all forms (from PP017 - PP019), the privacy statement and the imprint must be fully visible without horizontal scrolling. Text and images may protrude without limit in some cases, provided that not all text or images on a page protrude. For this inspection, all pages of the website to be certified and in particular the data protection declaration page, the imprint page and all pages containing forms must be examined.	In the mobile view of the Chrome Browser with 320 pixels display width, not all existing forms or the privacy statement page or the imprint page are fully visible without horizontal scrolling or all text or all images of a page protrude across the screen width.
Global additional inspection	Legally compliant execution of the web site with regard to integrations, extensions and	Optional inspection point	43	PP043	This inspection point is required if the number of employees is 50 or more or has been explicitly requested by an applicant with less than 50 employees. It is checked whether a confirmation is available that all required legally relevant	If this inspection point is required by the number of employees being 50 or more or if it is explicitly requested by an applicant with less than 50 employees. And if the list has not been submitted with the additional "Preliminary Work to be

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID	conform	non-conform[1]
	type of execution with regard to cyber security, GDPR, TMG.				mandatory information as well as the technical implementation in terms of cyber security, GDPR, TMG have been prepared professionally and appropriately. The website must be examined in all areas. The assessment and the confirmation of the successful implementation is issued by a trustworthy expert or consultant, as an independent person or organization. The applicant must provide the assessor/consultant with a comprehensible explanation of the experts or companies (or similar) who created the details on the website. If implementations were implemented also or exclusively by coworkers of the applicant, then the applicant can insure the professional creation informally, and this is recognized, if the consultant informed itself about the reliability and comprehensibleness of the insurance and can confirm. The basis of the insurance and confirmation is a list with details of all relevant legal and technical website areas that are relevant for the purpose of the appraisal. The list is to be submitted with the an additional "Preliminary Work to be Done" form and must be confirmed in writing by the assessor on	Done" form or the professional implementation has not been confirmed in writing by the assessor.

Inspec-tion area	Criterion	Extended notes for criterion	crite-ria num-ber	Crite-ria ID	conform	non-conform[1]
					the form as "professionally implemented according to available information".	

Notes and inspection requirements for the audit - Inspection list

- At the beginning of the audit the data and information must be checked or verified:
  - Are the details in the customer data application form and on the website consistent?
  - Is it a German company?
  - Is the company data complete and comprehensible?
  - Is it a web shop or a sales site?
  - Is the basic language in the areas to be examined German (except for additional English pages)?
- After the certification agreement has been concluded and before the audit, certain verification documents must be sent to the certifier for ownership (see Ownership Audit Area). Only when these are complete can the audit take place.
- The Chrome browser in its most current form must be used for the inspection.

[1] Non-conform results must always be documented internally in the form of a screenshot and also sent to the applicant with the notification of reasons. For the creation of screenshots please refer to Appendix 3 point 4 of the program manual.
[2] To make the complete URL including http:// or https:// visible when using the Chrome browser, double-click on the URL in the browser address line.
[3] DSGVO for DE with design extensions by the BDSG (Federal Data Protection Act) version from June 2019.
[4] HTTP cookie also known as web cookie, internet cookie, browser cookie or simply as a cookie.
[5] Opting out means expressing a contradiction. In the case of the cookie hint, you can object to the use of cookies by clicking the Opt-Out button.
[6] Opt-in means expressing consent. In the case of the cookie hint, you can agree to the use of cookies by clicking the opt-in button.
[7] Contact details are the same as company details in the imprint.
[8] A form is an area with input fields which are sent by clicking on a labelled button.
[9] As pages, all web pages with a unique URL are meant.
[10] Registered company legal form presented as: sole proprietorship, GbR, UG, GmbH, gGmbH, KG, eG, AG, e.V., sideline, Ltd., foundation.
[11] Sales pages are web pages on which a web shop is available or other sales against payment, which are operated with price information, ordering procedures.

5.4.2 IWTS-STANDARD VARIANT INTERNATIONAL

Inspection area	**Criterion**	**Extended notes for criterion**	**criteria number**	**Criteria ID Int.**	Based on criteria ID Dtl.	**conform**	**non-conform**[1]
Cyber Security	URL test	No open redirection to other URL after calling the operator web page URL	1	PE001	PP001	The URL specified in the application for certification does not change when it is called up in the browser (no forwarding).	The URL specified in the application for certification changes after it is called up in a browser (redirection).
	https:// URL	Hypertext Transfer Protocol Secure (HTTPS)	2	PE002	PP002	The URL called up in the browser first shows these 8 characters, starting from the beginning: https:// The result is to be documented by a screenshot (see program manual appendix 3 point 4).	The 8 characters https:// are not displayed first from the front or are not clear.
	SSL/TLS - Secure Sockets Layer/Transport Layer Security Encryption	Functional test SSL/TLS certificate Communication protocol Transport Layer Security, strong encryption of the communication protocol	3	PE003	PP003	The SSL/TLS certificate is tested with the Comodo SSL Checker tool (https://comodosslstore.com/ssltools/ssl-checker.php) and the SSL Labs SSL Server Test tool (https://www.ssllabs.com/ssltest) and the result contains no security or warning messages (the overall results are green). The result is to be documented by a screenshot (see program manual appendix 3 point 4).	The SSL/TLS certificate is tested with the Comodo SSL Checker tool and the SSL Labs SSL Server Test tool and the result shows at least one security or warning message (both or one of the overall results are marked red/orange).

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID Int.	Based on criteria ID Dtl.	conform	non-conform[1]
	Technical safety test	Checking the website for currently known and relevant malicious systems, malware and security holes (including malware, viruses, official blacklists)	4	PE019	PP042	Checking the website with the "Sucuri Site Check" tool (https://sitecheck.sucuri.net/) produces an overall result of only a "minimal" or at most "low" risk and is therefore green in each case. The result is to be documented by a screenshot (see program manual appendix 3 point 4).	Checking the website with the "Sucuri Site Check" tool gives an overall result higher than "low risk" and is therefore orange or red.
Data protection	Web contact form/s: Personal data collection	No blanket data collection, no blanket mandatory fields	5	PE004	PP019	Only necessary data such as salutation, name, e-mail address, subject and text message are requested in a contact form through defined mandatory fields. All other requested data must not be mandatory fields. If it is a newsletter subscription, only the e-mail field may be a mandatory field. For this inspection, all pages[9] of the website to be certified must be searched for forms.	In a contact form, in addition to the data or questions such as salutation, name, e-mail address, subject, text message or, in the case of a newsletter registration, in addition to the e-mail field, further data are requested which are marked as mandatory fields or without whose entry the sending of the form/registration is technically prevented. For this inspection, all pages of the website to be certified must be searched for forms.
Ownership	Domain ownership or right of use	Permission URL usage	6	PE005	PP025	The Customer has confirmed in the work order form that he has deposited the key for the domain holder verification and the	The customer has not stored a key or a key that differs from the order protocol

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID Int.	Based on criteria ID Dtl.	conform	non-conform[1]
		Preliminary document				Customer has deposited the key shown to him in the order protocol in the form "iwts-site-verification-[Key]" in the DNS report of his domain or server host and the verification with the tool Qualidator DNS Report (https://www.qualidator.com/WQM/de/Tools/DNSReport.aspx) confirms that the key has been deposited. The result of the test result with the DNS Report Tool must be documented by means of a screenshot (see program manual Appendix 3, point 4).	in the DNS report of his domain or server host.
	Ownership Verification Register extract	Optional inspection point Preliminary documentsError	7	PE006	PP026	Either the applicant has indicated in the application that he is subject to the obligation to register and has sent a document "extract from the register" in advance. Then check whether the company, owner, address and registration data of the document correspond with the data on the website to be certified. Or the applicant has indicated in the application that he is not required to be registered.	Either the applicant has indicated in the application that he/she is subject to the obligation to register but has not sent an "extract from the register" document in advance. Or the applicant has indicated in the application that he is subject to the obligation to register and has sent a document "extract from the register" in advance. However, the company, owner, address or registration data in the document do not match the data on the website to be certified.
	Ownership Verification	Optional inspection point	8	PE007	PP027	This inspection point is only relevant if the applicant has indicated in inspection point	This inspection point is only relevant if the applicant has indicated in inspection

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID Int.	Based on criteria ID Dtl.	conform	non-conform[1]
	Business registration	Preliminary documentsError				PP026 that he is not subject to registration: Either the applicant has indicated in the application that he/she is obliged to register a trade and has sent a "trade registration" document in advance. Then check whether the company, owner, address and registration data of the document correspond with the data on the website to be certified. Or the applicant has stated in the application that he is not required to register a business.	point PP026 that he is not subject to registration: Either the applicant has stated in the application that he is obliged to register a trade but has not sent a document "Trade Registration" in advance. Or the applicant has indicated in the application that he/she is obliged to register a trade and has sent a document "Trade Registration" in advance. However, the company, owner, address or registration data in the document do not match the data on the website to be certified.
	Ownership Verification Invoice document	Optional inspection point Preliminary documentsError	9	PE008	PP028	This inspection point is only relevant if no other document corresponding to inspection points PE006 or PE007 is available: It is necessary to check whether a document "invoice document" has been sent in advance and whether the applicant's company, owner and address registration data correspond to the information on the website.	This inspection point is only relevant if there is no other document corresponding to inspection points PP006 or PP007: The document does not exist or one or more data entries are not identical or missing.
	Imprint: Note	Unambiguous possibility of perception	10	PE009	PP029	On any web page of the domain to be checked, in the header (top) or footer (bottom), a link with the name "Imprint" is clearly visible, which links to the imprint	There is no clearly visible link in the header (top) or footer (bottom) of any web page of the domain to be checked, nor is a link with the designation

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID Int.	Based on criteria ID Dtl.	conform	non-conform[1]
						page. Alternatively, the complete imprint information can be displayed clearly visible on each page instead, as required in inspection points PE011 to PE017. The result of a page is to be documented by a screenshot (see program manual appendix 3 point 4).	"Imprint" or the complete imprint information, as required in inspection points PE011 to PE017.
	Imprint: Forwarding link to the imprint page	Link to imprint page available	11	PE010	PP030	When clicking also the link "Imprint", a new area or a new page with the designation Imprint and the imprint content must be visible. Result of the complete imprint is to be documented by screenshot (program manual appendix 3 point 4 to be observed).	If you also click on the link "Imprint" the imprint data is not visible.
	Imprint: Owner data/company information	Mandatory data Owner data	12	PE011	PP031	The information on company name, owner first and last name, address (street, house number, postcode, city) is available.	One or more mandatory details of the company are missing, such as: Company name, first and last name of the owner, address (street, number, postcode, city).
	Imprint: Registered company	Optional inspection point Verification whether it is	13	PE012	PP033	This inspection point is only relevant if the company of the website to be checked is a registered company, but not for individual companies: The applicant's indication in the certification application whether the applicant is a	The applicant has stated in the application that the company is a registered company (as a legal entity), but no excerpt from the register is available as a document copy, or the applicant has stated in the application that the company is not a registered company (as a

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID Int.	Based on criteria ID Dtl.	conform	non-conform[1]
		a legal person				registered legal entity was answered with "Yes" and an extract from the register, which the applicant has submitted, is available as a document copy.	legal entity), but the form of company stated in the imprint indicates that it is a registered company (as a legal entity).
	Imprint details: Legal form of the company in the case of a legal entity	Optional inspection point	14	PE013	PP034	In the case of legal persons, the company legal form9 must be written out in full or as an abbreviation after the company name.	The company is a legal entity, but the legal form is neither abbreviated nor written out in full after the company name.
	Imprint details: Contact possibility 1		15	PE014	PP035	One of the following contact options must be available: e-mail address, telephone number, fax number, contact form.	None of the following contact details are given: E-mail address, telephone number, fax number, contact form.
	Imprint details: Contact possibility 2		16	PE015	PP036	There must be another contact possibility (unequal to contact possibility 1): e-mail address, telephone number, fax number, contact form.	Only one or none of the contact details is given.
	Imprint details: Authorized representatives for legal persons	Optional inspection point	17	PE016	PP037	Indication of the first name and surname of the authorised representative.	The name of the authorised representative was incomplete or not given at all.
	Imprint details: Registration of legal entities	Optional inspection point	18	PE017	PP038	Indication of the registration number of the trade/association/partnership or cooperative register and the name and seat of the competent district court.	One, several or all details of the registration number or name or seat of the competent district court are missing.
User-friendliness	Responsive design: Recognizability of content on mobile devices	Mobile Version Responsive Test	19	PE018	PP041	The presence of the view in the Responsive Design is checked with Google's Chrome browser. To do this, switch to the mobile, responsive view in the developer tools in the Chrome browser (Menu ->	In the mobile view of the Chrome Browser with 320 pixels display width, not all existing forms or the privacy statement page or the imprint page are fully visible without horizontal scrolling

Inspection area	Criterion	Extended notes for criterion	criteria number	Criteria ID Int.	Based on criteria ID Dtl.	conform	non-conform[1]
						More tools -> Developer tools) and select a display width of 320 pixels (upper bar; view "Mobile S"). In the mobile view, all forms (from PE004), the privacy statement and the imprint must be fully visible without horizontal scrolling. Text and images may protrude without limit in some cases, provided that not all text or images on a page protrude. For this inspection, all pages of the website to be certified and in particular the data protection declaration page, the imprint page and all pages containing forms must be examined.	or all text or all images of a page protrude across the screen width.

<u>Notes and inspection requirements for the audit - Inspection list</u>

- At the beginning of the audit the data and information must be checked or verified:
  - Are the details in the customer data application form and on the website consistent?
  - Is the company data complete and comprehensible?
  - Is it a web shop or a sales site?
  - Is the basic language in the areas to be inspected German or English?
- After the certification agreement has been concluded and before the audit, certain verification documents must be sent to the certifier for ownership (see Ownership Audit Area). Only when these are complete can the audit take place.
- The Chrome browser in its most current form must be used for the inspection.

5.5 Contractual obligations between the parties

(a) A contract shall be concluded between the web site operator and the certification body before the first audit. Both sides are free in the design of this contract.

The contract should contain at least

- Rights and obligations of each contracting party
- Procedure of each side in case of detected non-compliance with individual criteria of the FdWB-Standard by the customer.
- Procedure in the event of infringements
- Termination clause
- Determination of remuneration
- The use of the conciliation office (advisory board of the FdWB) before legal action is taken.
- Furthermore all usual formal legal agreements.

Without restricting the freedom of contract, the following specifics of certification shall be included in the contract:

- *Regarding the termination clause*: With regard to its obligations, which it assumed with the recognition of the FdWB, the certification body will normally only terminate the contract if the customer has committed serious breaches of contract on several occasions.
  Applications for certification from applicants who have changed certification bodies several times at short notice and who are unable to provide the certification body with an acceptable justification for this change may be rejected due to high risk. In the event that the aforementioned risk has been covered up, the certification body may terminate the contract at any time with immediate effect.
  The certification body has the right to terminate the contract with immediate effect at any time in case of misuse of the certificate or the conformity mark. If the termination of the contract by the certification body was effected because the customer culpably violated his contractual obligations, the certification body is not liable for possible damages to the terminated company.
  With the valid termination of the contract, the certificate issued by the certification body and the authorization to use the logo expires. It must be removed from the website immediately. The certification body notifies the FdWB that the contract has been terminated. The FdWB initiates the shift in the certificate list from "valid certificates" to "terminated certificates".
- Regarding the *scale of fees*: The certification body sets its own scale of fees. This should contain at least the following information:
  - The list of fees indicates the fees for one calendar year for the complete execution of the certification procedure, consisting of the performance of audits, certifications and other individual services specific to the certification procedure.
  - Fees for audits (initial audit, follow-up audit, extraordinary audit)
  - Fee for preparation of the audit report
  - Fee for certification and delivery of the certificate
  - possibly other services

  It is possible to combine several or all fee elements into several partial flat rates or a total flat rate.

  The scale of fees must be submitted to the certification body at the program executing agency during the application procedure.

(b) Arrangements for cooperation between the certification body and the program owner shall be established by means of recognition or contract.

c) **NOTE**: There is no legal relationship between the certification client and the program owner. However, it is possible that a different legal relationship may arise between these two parties, e.g. in

their characteristics as professional association and website operator for professional advice or for association membership, etc.

5.6 Conditions for the granting of the certificate

The following conditions must be fulfilled for the granting of a certificate:

a) The certification body shall hold a valid accreditation by a national accreditation body and a valid licence from the program owner.

b) It has accepted the certification application of a website operator and a certification agreement with a website operator exists.

c) An auditor recognised by the certification body carried out an audit which showed conformity with the website criteria and the certification regulations.

d) In accordance with the dual control principle, a certifier recognized by the certification body made the certification decision.

e) The certificate must contain at least the following information:
   - Name of the certification body
   - Name of the certified program (If the program distinguishes several quality levels, the applicable quality level).
   - Mark of conformity (if national or regional versions of the program are used, the appropriate mark must be used)
   - Certification date
   - Signature of the certifier
   - Use of the conformity mark (logo) is permitted

5.7 Non-conformity with the FdWB-Standard

Non-conformity can have various reasons, e.g.

a) the customer has failed to comply with all criteria of the FdWB-Standard when setting up or changing his website,
b) the customer has failed to adapt all features of his website to changes in the FdWB-Standard,
c) the customer has created the impression by manipulation that his website is conform,
d) recertification has not been carried out (in time) through the fault of the customer.

If non-conformity is identified through an audit or through complaints from third parties about the non-conformity of the web site or through monitoring or other means, the certification body shall take the following actions:

a) During the audit the customer is informed verbally by the auditor, otherwise in writing by the certification body about the deviation.
b) Regardless of the reason for the deviation, the customer must remove the logo from the website immediately.
c) In case of minor non-conformity or low risk of non-conformity, the certification body shall provide the customer with a time limit for establishing conformity. This period shall be reasonable to correct the deviation itself or by involving third parties.
   After the notification of the production by the customer to the certification body, an unscheduled audit is carried out to establish conformity. Once this has been established, the logo may be placed again on the website.
d) In case of significant deviations or high risk, or is proceeded as in c). However, the certification body may temporarily declare the certificate invalid or withdraw it. The restoration of validity is effected by written notification to the customer. After withdrawal, a new initial audit is required to regain the certificate.
e) In case of very significant deviations or if the customer refuses to restore conformity, the program owner can inform the public about the certificate withdrawal via the "List of certificates".

If the withdrawal was due to serious fraud, the program owner may also publish the reason for the withdrawal.

5.8 Monitoring

If necessary, the program owner may order "monitoring" as defined in ISO ISO/IEC 17000:2004, 6.1 or ISO ISO/IEC 17067:2013, 5.3.7 Program type 5 at short notice. There are three ways of doing this:

a) by extension of the present IWTS program or
b) by authorization to instruct individual or all recognized certification bodies on the basis of the recognition granted to develop their own programs for monitoring all certificate users, to submit them to the Advisory Board for confirmation and to apply them, or
c) by authorising individual or all recognised certification bodies on the basis of the recognition granted to develop their own programs for monitoring certificate users with an increased risk level, to submit them to the Advisory Board for confirmation and to apply them.

The monitoring may only begin after it has been decided which of the methods a) to c) is to be used and the documents required for this have been approved by the advisory board.

NOTE: Surveillance means systematic repetition of conformity assessment activities as a basis for maintaining the validity of the statement of conformity. If monitoring is included, the
IWTS program shall define the set of activities (according to ISO/IEC 17067:2013 , Table 1, Function 6) that is part of the monitoring functions. When deciding on the appropriate monitoring activities, the program owner should take into account the nature of the product, the consequences and likelihood of non-conform products and the frequency of the activities.

5.9 Ensuring transparency at all levels

Transparency is ensured at all levels of the IWTS certification program.

To this end, the parties concerned shall freely make available to the other parties entitled thereto all information necessary to ensure the functioning of the system.

In addition, the program owner will ensure that the public and other possible interested parties are informed about the IWTS program in a transparent manner and that its reputation as an exemplary good web security system is promoted at all times.

5.10 Opposition and conciliation procedures

Certified companies and those companies that have applied for certification may, if no agreement can be reached with the complaints procedure of the certification body, file an appeal against the certification body with the advisory board of the FdWB, as conciliation body, against the following decisions:

a) Refusal to conclude a contract for the certification procedure,
b) Order additional audits,
c) Order more frequent audits in connection with higher risk ratings,
d) Refusal of certification,
e) withdrawal of the certificate.

The complaint shall be lodged stating the grounds on which the rights of the complainant company are alleged to have been infringed.

The Advisory Board shall decide within two weeks on the admissibility of the appeal. Persons directly affected by the decision are not involved in the decision-making process.

According to chapter 5.5 of this handbook, the advisory board should have been called upon as a conciliation body and should have made its decision before legal action is taken.

The Advisory Board also arbitrates in the event of disagreements regarding the interpretation in the IWTS program.

5.11 Record keeping

All participants in the IWTS program are obliged to archive the documents they are required to keep. The following obligations apply in particular:

a) The ***program owner*** archives all versions of his program for at least 10 years, this also applies to the documentation of the "program adaptations" (Appendix 1).

b) The ***certification bodies*** archive
   i. all relevant documentation on *accreditation* and *recognition of* program owners for at least 5 years,
   ii. all documents relating to *customer relations* (application form, contract, audit documents, including correspondence on deviations and payment defaults, certificates) etc. for 3 years In case of cancellations, the documents are archived for up to 3 years after the cancellation date.

The removal of archived documents or the deletion of digital memories must be carried out in compliance with the regulations on the flow of information and confidentiality as well as the regulations specified by law.

5.12 Marketing of the program

The marketing of the IWTS program is the responsibility of the program owner. All the usual marketing channels are freely available to him.

The program owner authorises the recognised certification bodies to use all their usual channels to draw public attention to the fact that they are involved in the certification of the IWTS program.

Program sponsors and each individual certification body will coordinate their marketing activities in such a way that the marketing of the program is optimised.

Clients certified against the IWTS program may support the marketing of the IWTS program within the scope of their interests.

5.13 Information flow ..... and confidentiality

With the exceptions listed below, all data and information exchanged during the certification process shall be treated confidentially. That is,

- digitally transmitted data and information,
- data and information stored on paper and other media, and
- verbally transmitted information

must be protected.

For digital data, this means that only secure data carriers and secure data transmission procedures may be used. Offices and other rooms in which confidential data is stored must be technically secured. The access of unauthorized persons to these rooms must be excluded. The parties involved in the IWTS program shall, where necessary, conclude appropriate agreements on data protection, which shall also include provisions on damages. The program owner does not accept any warranty claims for corresponding damages.

The destruction of files no longer requiring archiving and equivalent digital files must be carried out in such a way that secrets cannot be disclosed.

Excluded from confidentiality is the publication of

- users of forged certificates and
- Users of expired or withdrawn certificates.

Information about these invalid certificates is published in a separate section of all IWTS certificates on the Internet.

5.14 Proposals for improvement

All those involved in the IWTS program are invited to submit to the program owner any suggestions for improvement resulting from the practical application. The advisory board will evaluate these

proposals and decide what will be implemented. There is no entitlement to have submitted proposals implemented.

5.15 Property rights

The rights for the word/picture trademark of the IWTS certification program are held by the FdWB.

6 Duties and responsibilities of the parties involved

6.1 Roles and responsibilities of certified companies

6.1.1 CREATE AND MAINTAIN CONFORM WEBSITE

The customer is responsible for ensuring that his website is always in conformity with the IWTS standard (chapter 4.2 of this manual).

In preparation for the first audit, the interested party should obtain information about the requirements of the IWTS standard for his website and determine the degree of conformity by means of a self-assessment. In the case of remaining deviations, he should have them eliminated (or have them eliminated) before the audit. For this purpose he may seek advice from third parties.

During the first audit, the interested party is solely responsible for the full conformity of all product requirements (chapter 5.4) and certification requirements (chapters 5.5 to 5.15 and in the contract with the certification company). Any deficits identified shall be solely at his expense, irrespective of the causes of the defect. This may also mean that he has to carry out rework and that the granting of the certificate is suspended until such time as the rework has led to full conformity.

While the website operator is in possession of a valid certificate, he is responsible for ensuring that conformity with the requirements of the IWTS program is always guaranteed. This includes that he has to inform himself about possible changes in the criteria and implement this on his website.

The certificate user is obliged to notify the certification body with which he is contractually bound immediately of any changes to his website or company that may affect conformity with the program criteria.

The certificate user is recommended to remove the logo from the website for this period of time in case his website suddenly and not only for a very short time does not guarantee conformity due to special circumstances, in order to avoid possible damages to third parties.

After suspension or withdrawal of the certificate, the website operator will inform his existing customers in writing about the withdrawal in order to ensure that no damage can occur to third parties.

The website operator grants the auditor access to the website on the agreed audit date in order to be able to check all criteria of the FdWB-Standard for conformity. Refusals of access that lead to a new audit appointment and thus cause extra costs can be passed on to the website operator.

The website operator guarantees that he himself or a responsible employee will be available to the auditor for any queries regarding the audit result.

The web site operator is obliged to eliminate or have eliminated any deviations and deficits found during the audit within the time limit set by the certification body and to inform the certification body of the completion.

The website operator shall keep all inspection documents for at least 5 years. The FdWB grants the Certification Body access to documents in the past at any time and grants the FdWB or its bodies the same rights as the Certification Body.

The web site operator has the right to refuse an auditor or an audit if he can justify that he considers the criteria of objectivity, neutrality and impartiality required in this manual and/or the obligation of confidentiality to be not assured by the auditor or the certification body. He is also entitled to do so if

he suspects that the control procedure has not been carried out properly. He must inform the head of the inspection body in writing of such refusal.

The website operator has the right to appeal to the steering committee of the certification body in case of questions, suggestions, complaints, objections and disputes concerning the certification procedure.

The website operator has the right to submit a complaint to the Arbitration Board of the FdWB in the event of an improperly handled complaint to the Certification Body.

All the information required in the certification procedure between the company, the inspection body and the association will be forwarded only to the competent association bodies.

6.1.2 Application to certification body

Interested website operators submit a form-based application (Annex 2) for certification to a certification body recognised by the program owner. This is available from the recognised certification bodies. With the approval of the application and the signing of a certification contract between the client (client) and the certification body, all legal requirements for the certification process are met.

6.1.3 Fees for the certification procedure

Each certification body creates its own fee table for its services to its customers (= website operators). The Program Guide provides a framework for the certification bodies' fee tables. In the event of a dispute, the contract concluded between the client and the certification body is exclusively authoritative.

The table of fees should contain at least

a) The client undertakes to reimburse all costs incurred in connection with the certification procedures on the basis of the scale of fees and charges, which in its currently valid version forms part of the contract, in accordance with the invoices of the certification body.
b) Fees are charged for all certification activities depending on the actual effort involved. The basis for the calculation of the fees are
    i. the cost of audits and certification,
    ii. the classification of the enterprise in size/turnover classes,
    iii. Travel days and expenses: Certification/registration bodies are encouraged to reduce and share such costs between customers in the same geographical area, i.e. they are encouraged to combine and share on-site visits to customers in one geographical area where possible.
    iv. Flat rates for services directly related to certification.
c) The customer receives an invoice for the service rendered. Payments must be made without deduction within 2 weeks to the account of the certification body stated in the contract.
d) If payment is delayed, the certification body may suspend the certificate after the 2nd reminder. The customer must then remove the logo from his website until a valid certificate is reissued.
e) The certification body may unilaterally adjust the fees if the scope or location of activities changes during the current calendar year. Registered companies are obliged to notify the certification body of any operational changes that affect compliance with the criteria of the standard.

In order to save administrative costs, the certification bodies must collect any fees that may arise from the program owner (e.g. licenses or similar) with the certification invoice and pay them to the program owner. All additional agreements become part of the recognition contract.

6.1.4 Notification of substantial changes to the website

The customer is obliged to notify the certification body immediately if significant changes have been made to the certified website which could lead to non-conformity with the certificate issued.

If it becomes apparent through certain circumstances (e.g. reports from website users or competitors or through monitoring) that someone has suffered a loss due to the failure to report, the customer is solely responsible for this.

6.1.5 Use of the conformity mark

Certified website operators are granted the right to place the conformity mark (logo) on their website free of charge in order to clearly and easily communicate the commercial added value of their website to users of their website. Certificate users are also allowed to mark other documents related to the certificate with the logo.

Note: It is not allowed for certificate users to use the logo in contexts that have no direct connection to the certified website. Example: A mechanical engineering company whose website has been successfully certified under the YXZ program may not place the logo on its stationery or on promotional materials for its products.

Once the certificate has become invalid (for whatever reason), the certificate user must delete the logo from their website and may no longer distribute documents marked with the logo.

The program owner may grant certification bodies whose website has successfully passed an inspection similar to an IWTS permission to mark the certification body's website with the logo.

The certification bodies are allowed to mark with the logo, free of charge, those parts of their websites that are related to the IWTS program and all similar documents.

The program owner, who is also the rights holder to the logo, may use the logo for his or her purposes as he or she wishes.

6.1.6 Transparency

Certificate holders actively contribute to the transparency of the IWTS program on two levels:

a) They use all information possibilities available in the system to be informed at any time about the certification requirements for their website in such a way that deviations from the FdWB-Standard are avoided.
b) They shall provide the certification body with all information freely and controllably at the time of need, so that the certification body can establish conformity with the scheme without hindrance.

6.1.7 Termination

The certificate holder has the possibility to cancel his participation in the IWTS certification program at any time with the certification body. Outstanding payments to the certification body must be settled despite termination.

6.2 Tasks and responsibilities of certification bodies

6.2.1 Recognition requirements

The certification body must have a number of organizational, technical and legal prerequisites in order to be recognized by the program owner as a certification body for the IWTS program upon application to the program owner. In particular these are:

a) Fulfilment of the requirements for conformity assessment bodies according to ISIO 17065, which are confirmed by valid accreditation with a national accreditation body
b) Application of a quality management manual ("Manual of Procedures") describing the processes that the certification/registration body carries out in order to operate in conformity with ISO 17065,
c) a program manual related to the certification body, which describes the processes the certification body carries out in order to operate in conformity with the program manual of the FdWB,
d) Rules for the continuous assurance of the professional competence of the personnel working for the IWTS program in the certification body (acquisition and maintenance of competence),

e) Rules for the permanent guarantee of the personal prerequisites of the personnel working for the IWTS program in the certification body (neutrality, independence, ability to work with clients in a risk-oriented manner in stressful situations)
f) capable of acting management,
g) secured office space, which also provides a secure guarantee for data and secret protection,
h) financial resources that guarantee that the certification activity is carried out permanently and reliably for the contractually bound customers.

6.2.2 Certification application by interested website operators

Web site operators wishing to be certified against the IWTS program shall submit a form-based application to a certification body recognised for this program in accordance with the relevant provision of ISO 17065 (application form as Annex 2).

6.2.3 Audit execution

Audits are conducted to determine the conformity of a client's website with the IWTS program.

In every regular audit, the conformity of *all* criteria of the currently valid FdWB-Standard must be completely inspected. Deviations must be documented individually:

- Which criterion is not conform? Mention of the criteria number of the FdWB-Standard).
- What type of deviation was detected?
- Period until the customer eliminates the deviation.

Audits can be carried out by

1. An auditor recognised by the certification body for the IWTS program

or

2. by appropriate technical means

or

3. by a combination of a) and b).

In any case, the requirements for neutrality, independence and quality of testing and evaluation as specified in ISO 17000, ISO 17065, ISO 17067 and ISO 19011 shall be met.

Non-regular audits may be carried out at any time if the certification body has a reasonable suspicion of irregularities. These must always be reported to the company, stating the reasons for suspicion.

6.2.4 Implementation of certification (audit, certification, deviations, validity)

The certification is carried out by a certifier recognised by the certification company. He must take this into account in his decision:

a) the conformity of the audited website with all criteria of the FdWB-Standard, which is determined by the audit,
b) the conformity with the requirements of the certification scheme to be established by the certifier,
c) the conformity with the requirements of the certification body to be established by the certifier.

If all the requirements are met, the certificate is issued by the certifier and documented by issuing the certificate document.

If individual requirements from a) to c) are not in conformity, the certifier must grant the customer time limits for establishing conformity, stating the deviations found. In simple cases, the successful elimination of the deviations can be determined by the certifier, which then leads to the issue of the certificate.
In complicated cases, a further audit may be required to establish conformity and issue the certificate by the certifier.

As long as all requirements from a) to c) are not completely fulfilled, no certificate can be issued.

The certificate is valid

a) until the next regular audit, usually 12 months,
b) until non-conformity is detected, e.g. by complaints from third parties or by extraordinary audits due to the risk level or corresponding results of monitoring (if monitoring is ordered by the program owner (Chapter 5.8),
c) on withdrawal of the certificate by the certification body,
d) when the termination of the certification agreement takes effect.

6.2.5 Regular and extraordinary audits

In principle, the websites of all customers should be audited regularly every year (every 12 months).

The following deviations from this may be made by the certification body if the situation is determined by the certification body itself:

- The websites of individual customers can, for example, after the elimination of deviations identified in the audit, be additionally checked once to determine the success of the elimination. If necessary, additional one-off audits may be carried out until conformity has been demonstrated.
- The websites of individual clients may be audited in addition to the annual audit if there are any third party notifications to the certification body about this website that the website is not conform.
- If, as a result of changes in legal regulations or changes in standards, certain criteria of the FdWB-Standard have been changed in such a way that the implementation must be effective before the next audit, additional audits can be carried out for all affected websites after the change in standards has become effective.
- Individual additional audits may also be ordered if certain risks could arise for the users of this website.

The contract between the certification body and the client shall be concluded in such a way that the client is responsible for all costs of all audits. If a customer has the impression that certain audits have been incorrectly ordered or carried out by the certification body, he has the right of appeal (chapter 5.10).

6.2.6 Ensuring transparency

The certification bodies guarantee free transparency for the customers regarding the basics and the functions of the IWTS certification program as well as its application by the customer.

6.2.7 Withdrawal of certification

In the event of serious violations of the provisions of this Program Guide or of the certification agreement with the certification body, the certificate may be withdrawn from the client by the certification body. The customer concerned must be heard before the withdrawal. If he is not able to do so within 6 days, the withdrawal will be made immediately. A retroactive withdrawal of a certificate is not possible.

The customer must remove the logo of the IWTS program from his website immediately after withdrawal.

If the company from which the certificate has been withdrawn suffers economic or other damage as a result of the withdrawal, the certification body shall only be liable for this if it has culpably breached its obligations. The maximum amount of damage is limited to 10 times the annual certification fee.

If the withdrawal of the certificate causes damage to third parties, e.g. customers of the certified company, the website operator from whom the certificate was withdrawn in accordance with the regulations is liable.

6.2.8 REPORTING OBLIGATIONS TO THE PROGRAM OWNER

The program owner has the right to request from the recognized certification bodies certain reports on the functioning of the certification process, e.g. new customer acquisition, cancellations, number of certificates issued, number of deviations, number of complaints, etc.). The scope of the report should be limited to the minimum necessary for the functioning of the system. The reporting obligations are defined in the recognition procedure and documented in the letter of recognition.

6.3 Tasks *and responsibilities* of the program owner

6.3.1 PUBLIC RELATIONS

The program owner will regularly carry out qualified public relations work for the IWTS program. He uses his website, flyers, events and other suitable media and forms for this purpose. It covers all geographical areas where certification bodies operate.

The program owner implements public communication to make his program known and promote its use.

At least two target groups are formed and informed in a target group-specific manner (separation of target groups on the program website):

a) Public generally interested in website certification. For this purpose, website operators can also be considered assigned as long as they are not yet in the certification process. The content focuses on education about the benefits of the certification program and its certificate. The information offered is relatively static. Media are e.g. program website, brochures, public conferences etc.
b) Users of the certification program. This includes the certificate users and certification authorities. The content focuses on practical application topics. The information provided must be flexible and react very quickly to news about the program and its social environment. Media are e.g. program website, newsletter, consulting services.

The program owner will inform the recognised certification bodies in good time in advance about special actions so that they are prepared to react with their own actions if necessary.

6.3.2 INFORMATION TO PARTICIPANTS IN THE PROGRAM

The program owner will set up and operate a stable information system to transmit internal information to all program stakeholders. This could be, for example, a monthly (or on-demand) internet newsletter to all subscribed participants reporting on new developments in the program. The internal information service does not contain any confidential information. It is free of charge for the users.

6.3.3 INFORMATION AND ADVICE FOR INTERESTED PARTIES AND CUSTOMERS

The program owner provides information and advice to interested parties and customers in accordance with chapter 3 of this manual. He is completely free in the design of this task.

The program owner will consult with interested certification bodies that provide customer information on the certification program (no consulting according to chapter 3 of the handbook) on general questions in order to provide a concerted approach to interested parties and customers.

6.3.4 RECOGNITION OF CERTIFICATION BODIES

The program owner can recognise interested certification procedures in a formalised recognition procedure to work for the IWTS program.
Certification bodies must submit a formal application in writing to the program owner.

In the application procedure, the certification body must prove to the program owner that it fulfills the recognition requirements (chapter 6.2.1).

If the applicant certification body meets the requirements, the program owner can grant recognition. In the letter of recognition, the applicant may specify further program-related details that the certification body must comply with in applying its program. According to the principle of transparency and neutrality, these details should be identical for all certification bodies. Exceptions require a written justification to the advisory board.

Both the program owner and the certification body have a right of termination.

6.3.5 Updating the program

The updating of the program serves to maintain, improve and adapt the program to changing conditions inside and outside the program. To this end, the program owner should set up a procedure from which he can regularly obtain information from the stakeholders and interested parties on the acceptance of the program and on requests for its improvement. These should be evaluated to determine what remains unchanged and what should be improved.

The analysis should cover both program requirements and certification requirements (see, where applicable, under Terms of Reference, Chapter 3.).

a) Program requirements: Here, the validity and completeness of the FdWB-Standard (=criteria of the complete program) can be observed continuously. Special attention must be paid to whether certain standards and other normative documents have been changed or have become invalid, which has an influence on the FdWB-Standard.
b) Certification requirements: Here, the management and steering of the program, in particular the program adjustments, as well as the satisfaction of the certification bodies, the customers and the interested parties can be observed.
c) The program owner shall monitor that all certification bodies are operating uniformly according to the methods and procedures prescribed by the program manual to ensure consistency of results from the conformity assessment process of all clients.

The measures named under a) to c) must be formulated in writing as "program adjustments" in the first step (sample form as Annex 1) and sent to all certification bodies and customers. The program adaptations shall be dated and numbered consecutively to allow all parties concerned to monitor the completeness of the program adaptations themselves. In the second step, they are then to be sent to all parties involved in a timely and appropriate manner (e.g. newsletter by email) free of charge.

6.3.6 Rules on transparency

The program owner makes sure that he prepares and implements his own measures with maximum transparency in order to ensure the continuous satisfaction of the certification bodies, customers and interested parties.

6.3.7 Public directory of all certificates

The program owner keeps an up-to-date list of all IWTS certificates and publishes it on the Internet. In the recognition procedure (see Section 6.3.4), the certification authorities are required to send a corresponding message to the program owner when sending the certificate to the Web site operator. At the same place where valid certificates are published on the Internet, known certificates of the following categories are also published: invalid, revoked, forged.

6.3.8 Cooperation with other certification schemes or systems

Should similar certification programs or systems for the evaluation of websites become established on the market, the FdWB *can* enter into suitable cooperation with interested program owners for mutual benefit. This can be the avoidance of duplicate certification, where each certification scheme

contains elements that are of high value to users, but also elements that duplicate each other. The opposite is the cost-effective closing of gaps in your own program.
Example: Mutual recognition of certificates for precisely defined criteria groups. This allows the certificate user to extend the range of information provided by his certificate without increasing costs proportionally.
In any case, this requires qualified benchmarking, which should also include the reputation of the other program and its owner.

7. Normative references

(a) website security:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (basic data protection regulation)
- Regulation on the requirements for comparison websites under the Payment Accounts Act and for accreditation and conformity assessment (Regulation on comparison websites - VglWebV) of 16 July 2018 (Federal Law Gazette I p. 1182)
- Information technology - IT security procedures - Information security management systems - Requirements (DIN ISO/IEC 27001:2015-03)

Inspection area	**Criterion**	**Criteria ID Dtl.**	**Criteria ID Int.**	**Source**
Cyber Security	URL test	PP001	PE001	FdWB-Standard
	https:// URL	PP002	PE002	FdWB-Standard
	SSL/TLS - Secure Sockets Layer/Transport Layer Security Encryption	PP003	PE003	https://de.wikipedia.org/wiki/Transport_Layer_Security andhttps://de.wikibooks.org/wiki/IT-Sicherheit_f%C3%BCr_Privatanwender:_Grunds%C3%A4tze:_Transportverschl%C3%BCsselung
	Technical safety test	PP042	PE019	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
Data protection	HTTP cookie** present	PP004	-	https://www.gesetze-im-internet.de/tmg/__15.html andhttps://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html andhttp://curia.europa.eu/juris/document/document.jsf?text=ocid=216555ageIndex=0oclang=DEode=reqir=cc=firstart=1id=4667410 and data protection obligations of the ePrivacy Directive 2002/58/EC ("Cookie Directive")
	Cookie hint text available?	PP005	-	https://www.gesetze-im-internet.de/tmg/__15.html andhttps://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html andhttps://datenschutz-generator.de/eugh-urteil-like-button-cookie-opt-in-abmahnbarkeit/
	Ability to refuse cookies	PP006	-	https://www.gesetze-im-internet.de/tmg/__15.html

Inspec-tion area	Criterion	Criteria ID Dtl.	Criteria ID Int.	Source
				andhttps://www.e-recht24.de/artikel/daten-schutz/8451-hinweispflicht-fuer-cookies.html andhttps://datenschutz-generator.de/eugh-ur-teil-like-button-cookie-opt-in-abmahnbarkeit/
	Possibility to allow cookies	PP007	-	https://www.gesetze-im-inter-net.de/tmg/__15.html andhttps://www.e-recht24.de/artikel/daten-schutz/8451-hinweispflicht-fuer-cookies.html andhttps://datenschutz-generator.de/eugh-ur-teil-like-button-cookie-opt-in-abmahnbarkeit/
	Link to privacy policy	PP008	-	https://www.bundestag.de/dokumente/textar-chiv/2019/kw26-de-datenschutz-649218
	Link to privacy policy - addi-tional pages in other lan-guages	PP009	-	https://www.datenschutz.org/datenschutzer-klaerung-mehrsprachig/
	Is there a pri-vacy policy?	PP010	-	https://www.bmwi.de/Redaktion/DE/Arti-kel/Digitale-Welt/europaeische-datenschutz-grundverordnung.html
	Is there a pri-vacy policy? - additional pages in other languages	PP011	-	FdWB-Standard
	Form of the privacy policy is clear and structured	PP012	-	FdWB-Standard
	Form of the privacy policy is clear and structured - additional pages in other languages	PP013	-	FdWB-Standard
	Data of the company in the privacy policy	PP014	-	https://www.bmwi.de/Redaktion/DE/Arti-kel/Digitale-Welt/europaeische-datenschutz-grundverordnung.html
	Company data in the privacy policy - pages in other lan-guages	PP015	-	FdWB-Standard

Inspection area	Criterion	Criteria ID Dtl.	Criteria ID Int.	Source
	Duty to inform data protection officers	PP016	-	https://www.bundestag.de/dokumente/textarchiv/2019/kw26-de-datenschutz-649218
	Web contact form(s): Privacy policy	PP017	-	https://www.e-recht24.de/dsgvo-gesetz.html andhttps://www.e-recht24.de/news/abmahnung/10651-abwarnung-kontaktformulare-einwilligung.html
	Web contact form(s): Privacy checkbox	PP018	-	https://www.e-recht24.de/dsgvo-gesetz.html andhttps://www.e-recht24.de/news/abmahnung/10651-abwarnung-kontaktformulare-einwilligung.html
	Web contact form/s: Personal data collection	PP019	PE004	https://www.e-recht24.de/dsgvo-gesetz.html andhttps://www.e-recht24.de/news/abmahnung/10651-abwarnung-kontaktformulare-einwilligung.html
	Right of access to information (personalised data)	PP020	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
	Right of access refusal (personalised data)	PP021	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
	Consent to data processing by third parties (personalised data)	PP022	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
	Secure data transmission (on the Internet)	PP023	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
	No blanket data collection (with forms)	PP024	-	https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Aufbau_der_DSGVO
Ownership	Domain ownership or right of use	PP025	PE005	https://www.denic.de/webwhois/
	Ownership Verification Register extract	PP026	PE006	FdWB-Standard
	Ownership Verification Business registration	PP027	PE007	FdWB-Standard

Inspec-tion area	Criterion	Criteria ID Dtl.	Criteria ID Int.	Source
	Ownership Verification Invoice document	PP028	PE008	FdWB-Standard
	Imprint: Note	PP029	PE009	Telemedia Act (TMG) § 5 General information duties andhttps://www.gesetze-im-internet.de/tmg/__5.html
	Imprint: Forwarding link to the imprint page	PP030	PE010	Telemedia Act (TMG) § 5 General information duties andhttps://www.gesetze-im-internet.de/tmg/__5.html
	Imprint: Owner data/company information	PP031	PE011	Telemedia Act (TMG) § 5 General information duties andhttps://www.gesetze-im-internet.de/tmg/__5.html
	Imprint: Seat of the company	PP032	PE012	FdWB-Standard
	Imprint: Registered company	PP033	PE013	Telemedia Act (TMG) § 5 General information duties andhttps://www.gesetze-im-internet.de/tmg/__5.html
	Imprint details: Legal form of the company in the case of a legal entity	PP034	PE014	Telemedia Act (TMG) § 5 General information duties andhttps://www.gesetze-im-internet.de/tmg/__5.html
	Imprint details: Contact possibility 1	PP035	PE015	Telemedia Act (TMG) § 5 General information duties andhttps://www.gesetze-im-internet.de/tmg/__5.html
	Imprint details: Contact possibility 2	PP036	PE016	FdWB-Standard
	Imprint details: Authorized representatives for legal persons	PP037	PE017	Telemedia Act (TMG) § 5 General information duties andhttps://www.gesetze-im-internet.de/tmg/__5.html
	Imprint details:	PP038	PE018	Telemedia Act (TMG) § 5 General information duties

Inspec-tion area	Criterion	Criteria ID Dtl.	Criteria ID Int.	Source
	Registration of legal entities			andhttps://www.gesetze-im-inter-net.de/tmg/__5.html
	Imprint de-tails: Recogni-tion of certain professions	PP039	-	Telemedia Act (TMG) § 5 General Information Obligationsandhttps://www.gesetze-im-inter-net.de/tmg/__5.html
	Imprint de-tails: Internet shops/selling websites	PP040	-	Telemedia Act (TMG) § 5 General information duties andhttps://www.gesetze-im-inter-net.de/tmg/__5.html
User-friend-liness	Responsive design: Recog-nizability of content on mobile devices	PP041	PE019	FdWB-Standard

(b) Certification methodology

- 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]
- EN ISO/IEC 17000:2005-03 Conformity assessment - Terminology and general principles; Trilingual version EN ISO/IEC 17000:2004
- ISO/IEC 17007:2009-09 Conformity assessment - Guidelines for the development of appropriate normative documents for conformity assessment
- EN ISO/IEC 17030:2009 Conformity assessment - General requirements for third party conformity marking (ISO/IEC 17030:2003) German and English version EN ISO/IEC 17030:2009
- ISO/IEC 17065:2012-09 Conformity assessment - Requirements for bodies providing certification of products, processes and services
- DIN EN ISO/IEC 17067:2013-12 Conformity assessment - Principles of product certification and guidelines for product certification schemes (ISO/IEC 17067:2013); German and English version EN ISO/IEC 17067:201
- DIN EN ISO 19011:2018-10 Guidelines for the auditing of management systems (ISO 19011:2018); German and English version EN ISO 19011:2018

[1] "This standard was last reviewed and confirmed in 2014. Therefore this version is still up to date. "Source (June 2019): https://www.iso.org/standard/19736.html

Annexes

APPENDIX 1: SAMPLE FORM "PROGRAM ADJUSTMENT

Professional association of German website operators GmbH (FdWB)		
Program manual for the certification of websites according to the IWTS program		
Program version: Status: June 2019; Version: 0.0	Adaptation No: XX/2019	Date of issue: XX.XX. 2019
Subject: Chapter XX, paragraph XX, point XX	[Which part of the HB is to be changed?]	
Reason for change:	Description of the reason for the amendment, e.g. amendment of a standard or law or resolution of a process conflict; the amended standard, law or process conflict must be defined].	
Changed text:		
Valid from:	There should be sufficient time between the notification of the program adaptation to certification/registration bodies and certificate users to prepare the implementation in such a way that audits can be carried out fairly and completely on the day after the start of validity].	
Comments:		

APPENDIX 2: MODEL FOR THE APPLICATION FOR CERTIFICATION

The form for the certification application is designed by each certification body itself according to the contents specified in the model. She may make additions.

[Name of certification authority]	**Program manual the program IWTS**	**Section XX** **FM XX-XX**
Date: XX.XX. 20XX	version: 01	Page: 52 of 56

Application form
for inspection and certification under the scheme IWTS by the certification body [name]...

Name and legal form of the applicant company: (Please enter the full company name)	**Address of the company:** (street, house number, postal code, city, state, country, post office box)
Legal representative of the company: (Name and function)	**Contact person for IWTS certification:** (Please fill in, if not identical with the legal representative)
Phone: **Fax:** **Mobile:**	**E-mail:** **website:**

(Mark with a cross where applicable)

☐ **Initial application**

☐ **Change notification** (if you are already a customer of the certification body)

Please tick the appropriate version of the IWTS program

☐
☐
☐
☐
☐
☐

1. information about the company (industry, activity, locations)

4. Information about the website to be certified: Domain: Brief description: **5. Does your company have other websites that are not to be certified (Yes/No)**
4. have you ever been registered, audited or certified for the IWTS program by another certification body? If yes, please state: the name of the certification body, the year of application, the previous registration number, the reasons for the change.
6. Here you can provide further information or express special wishes that are relevant for the certification of your company, e.g. a more detailed description of your activity, the travel time between the different parts of the company (if applicable), etc. :
I, the undersigned, declare that the application form is completed accurately and in full **Name of the company: ……..** **Legal representative: …….** **Date ……** **Signature: …….**

APPENDIX 3 AUDIT PROCESS DESCRIPTION

Direct access: IWTS-Audit-Portal
(for auditors and certifiers): https://iwts-certificate.com/auditing-iwts/

1. Preparation
   a. The initial request for the audit is the audit deadline.
   b. Open the IWTS Audit Portal.
   c. View whether notifications of new versions, notes or inspection instructions are available in the IWTS portal.

2. Audit
   Check inspection requirements
   a. Login on the page Auditing IMTS with personal auditor/certifier password.
   b. Is the customer data from the application identical to the data in the inspection area (name, customer number, etc.) to be found under "Company data" on the right-hand side of the screen)?
   c. If to-do exists (recognizable status: to-do complete. You will find all links under "Contribute documents"?

3. Audit/Certification
   a. On the right hand side you will see all inspection points. When clicking on a inspection point, the variants "conforming" and "non-conforming" appear for adjustment.
   b. Enter your inspection result in the audit table (left side) with any comments
   c. Define the result of the audit/certification as a status in the field "Audit result" or "Certification result". The status can be:
      "Audit/Certification Waiting status" or "Audit/Certification is fully completed".
      If an exam is "non-conform" or if there are open or unresolved questions, then "wait status" must be set.

4. Screenshots
   To create suitable screenshots
   a. The screenshot should always document the subject of the inspection and if possible a reference to the inspected website (company name, domain, data, design).
   b. For example, save the screenshots in a local area.
   c. Change the screenshot file name:
      Customer number, order number, ID of the inspection point, number of screenshots per inspection point, A or Z (auditor or certifier), date.
      Example: 123456-23450-3-1-A-11092019.jpg
   d. After all inspection points have been executed, please upload (drag and drop) all screenshots in the field "Upload Screenshots-Au1".
   e. Attention: After adding the files, the upload must be started actively by clicking on the button "Start upload"!

5. Where do I find the testing tools:
   Audit page on the right, under the item "Audit Tools".

6. By clicking on "Send" the inspection is completed.
   Please check all entries beforehand.

7. Clues:
   Contact form on the right: Here you can send remarks, notes, errors or similar to the technical department.

   Our goal is to make this portal as user-friendly as possible. Please support us in this. If you have any comments or questions, please send us a message under Contact/Contact form.

APPENDIX 4: OVERVIEW OF THE TESTING TOOLS

Criterion	German Standard	International Standard	Testing Tools	
	Criteria ID	Criteria ID	Name	Link
SSL/TLS	PP003	PE003	Comodo SSL Checker	https://comodossls-tore.com/ssltools/ssl-checker.php
SSL/TLS	PP003	PE003	SSL Labs SSL Server Test	https://www.ssllabs.com/ssltest
safety engineering test	PP042	PE019	Sucuri Site Check	https://sitecheck.sucuri.net/
Cookies	PP004	-	Cookie-Metrix	https://www.cookie-metrix.com
Authorization URL usage	PP025	PE005	Qualidator DNS Report	https://www.qualidator.com/WQM/de/Tools/DNSReport.aspx
Headquarters	PP032	PE012	German Post	https://www.postdirekt.de/plzserver
Value added tax ID	PP040	-	Check sales tax ID	https://ust-id-pruefen.de