Management Service

Mehr Sicherheit.
Mehr Wert.

Requirements catalog

for the assessment and certification of tourist industry Internet offerings

(e.g. Internet travel agencies, tour-operator portals)

Version 3.8
As of: May 14, 2007

TÜV SÜD Management Service GmbH
Internet-Zertifizierungen s@fer-shopping
Ridlerstrasse 65
D-80339 Munich

Tel.: 089 / 57 91 - 43 00
Fax: 089 / 51 55 - 10 97
e-mail: info@safer-shopping.de
Internet: www.safer-shopping.de

Management Service

Contents

0 Management context 3
0.1 Commitment to satisfy requirements 3
0.2 Communication of requirements 3
0.3 Definition of responsibilities 3
0.4 Use of effective procedures 3
0.5 Provision of necessary resources 3
0.6 Conformity evaluation 3
0.7 Process and procedure optimization 3
1 Data security 3
1.1 Security scheme 3
1.2 Security measures 3
1.3 Handling of malfunctions and emergencies 4
2 Data protection 4
2.1 Data protection representative 4
2.2 Commitment to data security and privacy 4
2.3 Collection, processing and use of personal data 4
2.4 User information 4
2.5 Further data use 4
2.6 Use profiles 5
2.7 Use of cookies 5
2.8 Information about saved data 5
3 Online contents and processes 5
3.1 Restrictions concerning offerings and contents 5
3.2 Promotional offers 5
3.3 General information 5
3.4 Performance details, costs and other customer information 6
3.5 Selection and booking process 7
3.6 Payment process 7
3.7 Delivery of travel documentation 7
3.8 Customer service 8

Annex 1: External quotations

Annex 2: Disclaimer

0 Management context

0.1 Commitment to satisfy requirements

The employees responsible for the Internet offerings and business processes associated therewith are liable for satisfying all requirements of this catalog and all relevant statutory provisions. Proof that they have assumed this responsibility is provided by means of suitable measures.

0.2 Communication of requirements

Within the organization, the requirements outlined in this catalog are adequately communicated to all employees concerned.

0.3 Definition of responsibilities

Responsibilities and authorities in the organization have been clearly and completely defined in order to ensure satisfaction of all requirements. Suitable arrangements have been made regarding substitutes.

0.4 Use of effective procedures

Procedures suitable for implementing the requirements within the organization have been established. These procedures conform to the statements and contents of the Internet offerings.

0.5 Provision of necessary resources

Suitable resources for requirement satisfaction (e.g. trained personnel, necessary infrastructure) are made available.

0.6 Conformity evaluation

The organization assesses conformity in terms of requirement satisfaction. Customer satisfact-ion, above all, is assessed at regular intervals.

0.7 Process and procedure optimization

The results of the evaluation as per Article 0.6 above are used to optimize the pertinent processes and procedures.

1 Data security

1.1 Security scheme

The organization has established a suitable security scheme to ensure appropriate protection of the contents of the Internet offerings and the personal data of users and customers. The provider addresses possible threats. Protection objectives and requirements are defined and constantly updated. Appropriate security measures are defined on this basis.

1.2 Security measures

The security measures adequately counteract all relevant threats and correspond to the state of the art. All areas involved in business transactions, in as far as they can be influenced by the provider, need to be protected. This applies, above all, to processes carried out and facilities operated at the provider's organization or on behalf of the latter and data-transmission paths between provider and customer. For this purpose, the provider also takes the following measures:

a) security aspects are taken into account when personnel is selected (e.g. appropriate qualifications);

b) responsibility for the security of personal data has been clearly assigned and defined. Existing organizational framework conditions are adequately considered in this context;

c) systems and applications (e.g. web and application servers, databases, merchandise information and backoffice systems) have been professionally installed and their security standard is kept up to date;

d) security-relevant settings are thoroughly planned and comprehensible;

e) the installation of unapproved software is prohibited;

f) effective virus protection programs have been installed and activated;

g) access to personal customer data is safeguarded by suitable building infrastructure. Access authorizations have been regulated;

h) personal data may only be accessed by authenticated persons. The pertinent authorizations are granted in line with the relevant tasks (‘need to do’ principle);

i) data carriers containing personal data are stored securely;

j) personal data is backed up on a regular basis. In this context, the relevant data

protection provisions are observed (see also Chapter 2);

k) encryption technology is applied to ensure user privacy protection. Personal data can be entered in encrypted mode. As far as payment information is concerned, code lengths of at least 128 bits, for symmetrical encryption, and 768 bits – or even better 1024 bits – for asymmetric encryption, are used. Additionally, unencrypted data transmission may be offered where encrypted transmission is clearly recommended;

l) to ensure protection against attacks from the outside, a firewall or similar protection mechanism is used;

m) technical components (software or hardware) to be installed or special settings to be effected by the customer for the sake of business-transaction security are pointed out to the latter and the pertinent procedure is explained. System requirements are defined;

n) customers are informed about possible damage associated with program downloads.

1.3 Handling of malfunctions and emergencies

A consistent scheme for handling operating malfunctions and emergencies has been established. This scheme includes the names of the responsible persons and/or their roles and authorities.

2 Data protection

To ensure the protection of users' and customers' personal data, the relevant legal regulations must be adhered to (e.g. German Telemedia Act – ("Telemediengesetz"), Federal Data Protection Act ("Bundesdatenschutzgesetz"). The requirements outlined below must be observed in particular:

2.1 Data protection representative

A data protection representative must be appointed for organizations employing five employees or more who process personal data.

2.2 Commitment to data security and privacy

Employees in contact with personal data are liable for observing data security and privacy and have been instructed accordingly prior to taking up their activities.

2.3 Collection, processing and use of personal data

Without the user's agreement, personal data may only be collected, processed and used in as far as this is required for establishing, shaping or amending a contractual relationship. As soon as the above purpose no longer exists, the data will be deleted. Instead of deleting the data, it may also be blocked, should such data be subject to a statutory or contractual retention period.

Offerings addressing minors will not be used to record, evaluate or disclose to third parties any personal data of the minor users or of persons living in their households without prior information of and agreement by their legal guardians.

2.4 User information

Before any data is used, users will be informed about the type, scope and purpose of the collection, processing and use of personal data, unless such information has already been provided. It must be possible to call up this information at any time. The names of further data recipients, if any, will be provided.

Specific information about data processing should be provided in the context of the data collection.

2.5 Further data use

Personal data may only be used or processed for consulting, advertising and market-research purposes or to shape communication and information services in line with demand, if the respective user has expressly agreed thereto. Declarations of consent may be submitted electronically via clear and deliberate acts on the part of the user (e.g. by activating a checkbox). Declarations of consent are saved by legally prescribed technical and organizational measures and recorded. Users are informed, prior to declaring their consent, that they are entitled to withdraw the latter at any time. This information can be called up electronically by the user at any time.

2.6 Use profiles

Use profiles will only be generated either anonymously or using pseudonyms which cannot be traced back to their respective pseudonym carriers, unless the user has actively agreed to the preparation of such a profile. Users may have been informed in advance that they are entitled to object to this type of use of their data.

2.7 Use of cookies

Users will be informed specifically and comprehensibly about the use and functionality of any cookies employed. This information is mandatory, if cookies save and make it possible to call up data that may be traced back to individual persons. Online merchants also inform customers about the possible consequences, should they object to the use of cookies, and the risks of damage that may be associated with their deployment.

2.8 Information about saved data

The online merchant will inform customers free of charge and instantly about any data regarding their persons or pseudonyms that have been saved. At the customer's request, this information may also be provided electronically.

3 Online contents and processes

3.1 Restrictions concerning offerings and contents

Only offerings and contents complying with the statutory regulations are provided. Above all, the provisions of the Youth Protection Act (JuSchG) and the Interstate Treaty on Protection of Minors in the Media (JMStV) must be observed.

3.2 Promotional offers

Electronic offers used for promotional or similar purposes (e.g. special offers, competitions) must be clearly recognizable as such. The organization behind such offers must be clearly identifiable.

3.3 General information

The following general information will be made available to potential customers prior to contract conclusion:

a) Full name and identity of the online merchant:
   - name, address and legal form of the organization, location in which it has been registered and can be summoned;
   - in cases involving legal persons: name of the authorized representative;
   - depending on the provider's legal form, the number of the Commercial Register, Register of Associations, Register of Partnerships or Public Register of Cooperatives and the respectively competent court of register are quoted;
   - VAT identification number as per Article 27 a) of Value-Added-Tax Law, if any;
   - information about the competent supervisory authority (e.g. in cases involving travel insurance), where appropriate.

b) Online merchants should clearly define the national clientele they wish to address with their offerings. The language of their Internet pages may be freely selected. The language choice may represent a criterion for the target groups selected. If providers wish to restrict their clientele, they will make this clear via a list of countries, for example.

c) It should be easy to access, save or print the online merchant's General Terms and Conditions of Business. Their text should be clearly structured and easy to read for customers. Providers are responsible for ensuring that the General Terms and Conditions of Business they use correspond to the national law governing the contract in question. All information duties under these legal systems must be fulfilled in the respectively prescribed form. Customers will be informed whether the text of the contract will be saved by the online merchant after contract conclusion and be accessible to the customer.

d) Online merchants provide information about all relevant conduct codices to which they subscribe; they provide information on how these codices can be accessed electronically.

3.4 Service details, costs and other customer information

a) To enable potential customers to obtain a comprehensive picture of the services to be expected and the associated costs, the following information will be provided prior to contract conclusion:

- travel price, including all taxes and other price elements, and any mail costs that may also arise. Seasonal surcharges and discounts or other rebates and price reductions must also be quoted. (The price must include the booking fee to be paid but not the costs of travel cancellation insurance, variable fuel and cleaning costs or health resort tax. Air fares quoted must include airport fees and taxes.) If prices are broken down, the total must be highlighted;
- clear and comprehensible name of destination (generally, the geographical or administrative name of the destination is quoted);
- for rail, bus, air or sea journeys: more detailed classification (e.g. 1st or 2nd class, coach quality, charter, tourist or other class);
- type of accommodation (e.g. hotel, holiday home, club etc.), location, category or comfort, main characteristics and tourist classification (e.g. stars);
- type of board (e.g. no meals, accommodation plus breakfast, half-board or full-board). Information about special features such as breakfast buffet, menu selection or meals to be eaten in the hotel next door must be provided;
- for cruises and tours: information about the travel route, citing departure and destination airports and connections, if any;
- reference to information about passport, visa and statutory health requirements (e.g. compulsory vaccinations);
- required minimum number of participants for the journey to take place and the date prior to its contractually agreed start by which travelers must have been informed at the latest that the journey will have to be cancelled because the required minimum number of participants has not been reached;
- payment details, including comprehensive information about payment routes, provider's special terms and conditions of payment (e.g. special fees for payment procedure), transaction date in cases involving direct debits, credit-card payment or electronic payment.

b) After contract conclusion, customers will immediately receive a booking confirmation including the following information*: (this obligation to provide such information does not apply if the traveler books the journey less than 7 workdays before the start of the journey. Travelers must, however, always be informed about their obligations regarding notices of defects and the deadlines to be observed in line with Article 651 g German Civil Code (BGB). Tour operators may also fulfill their above obligations by referring to information included in the brochures issued and handed out to travelers. Booking confirmation must include the travel price and terms of payment, at all events).

- travel price and terms of payment and, in as far as significant for the type of the journey, information as outlined under a) above (transport, accommodation, board, travel route, minimum number of participants);
- final or individual destination(s), individual durations and pertinent dates;
- dates, anticipated time and place of departure and return;
- visits, excursions and other services included in the travel price;
- information as to whether the journey is subject to changes in price, the defining factors for such changes and price elements not included in the travel price;
- special wishes agreed with the traveler;
- tour operator's name and address;
- information about ways of terminating the contract and the pertinent deadlines (Article 651 g German Civil Code (BGB));

- information about the optional conclusion of a travel cancellation insurance to cover reimbursement in cases of accident or illness, stating name and address of the insurance company.

c) Prior to the journey, the customer will receive the following information: (should this information already be included in a brochure or booking confirmation, it does not have to be provided separately):

- departure and arrival times, stopovers and connections to be reached there;
- specific seat reservations, if travelers have to be seated in a certain place during transport;
- name(s), address(es) and phone number(s) of the tour operator's local representative or – if unavailable – of local bodies which can help travelers in case of difficulties. Should there be no such bodies, travelers must be provided with an emergency number and other information to assist them in contacting the tour operator.
- if minors are traveling abroad, the person whose name is cited on the booking (generally the legal guardian) must be informed about how he/she can directly contact the child or a responsible person at the child's place of residence.
- evidence of insolvency insurance including a Payment Security Certificate (proof of protection against tour-operator bankruptcy) as per Article 651 k German Civil Code (BGB) (for package tours).

3.5 Selection and booking process

The functions for searching, selecting and booking travel offerings are correct, transparent and user-friendly:

a) an overview of the services offered can be easily obtained;

b) the individual steps leading to contract conclusion are easy to recognize;

c) all relevant information (for example about providers, services, terms and conditions of booking, data protection) can be easily accessed. They are easy to understand and meaningfully presented;

d) queries regarding offerings and services are correctly executed; contents are logical and consistent;

e) all services selected by the user are summarized and the travel price is cited prior to booking;

f) when entering information, users can clearly recognize which entries are mandatory and which entries are optional;

g) incorrect entries can be recognized by the user and corrected;

h) users are well aware in advance of precisely when they will effect a booking and when a contract will be concluded. In this context, the fact that they are now about to make a booking and that their next "click" will result in contract conclusion is clear to users;

i) users can abort the booking process at any time without having effected a booking;

j) customers immediately receive a booking confirmation by e-mail.

3.6 Payment process

Basic payment functions are correct, transparent and easy to handle;

a) an overview of available payment procedures can be easily obtained;

b) details of the payment process (Article 3.4 a)) are easy to understand and meaningfully presented;

c) (electronic) payment is effected correctly and in line with the selection made;

d) customers receive a payment confirmation that is clearly assignable to the booking (e.g. clear identification on the bank statement).

3.7 Delivery of travel documents

The organization has established an effective procedure to ensure timely provision of all travel documents;

a) delivery is effected within the deadline defined to the customer;

b) should there be insufficient time to ensure punctual delivery of travel documents to the customer, they may also be provided in

a different manner (e.g. deposit at the airport).

3.8 Customer service

The online merchant offers appropriate customer service (e.g. assistance in using the online offerings, details regarding services, handling of booking and complaints):

a) customers can contact online merchants. In addition to an e-mail address, customers should also be provided with a telephone number to enable rapid contact;

b) customer queries and complaints are professionally answered within a reasonable period of time. The customer will be informed in advance should it not be possible to provide an answer within a short period of time;

c) if a journey has to be cancelled, the customer must be informed of this fact well in advance and alternatives offered;

Management Service

Annex 1: External offerings

Generally, online merchants in the tourist industry cooperate with a number of partners in front end transactions (integrated through external links). Depending on their tasks, these partners will be categorized differently and *s@fer-shopping*™ requirements for the partners will correlate with their specific tasks.

The following overview shows the different types of partners and the pertinent requirements:

Type of partner / task	**Requirements**
IBE (Internet Booking Engine) Tool for research and booking on the basis of the online merchant's agency terms and conditions of business	- With respect to external partners, data protection and security are guaranteed in writing and are plausible; - Personal data can be submitted in encrypted mode (e.g. SSL 128 bits). Appropriate protection of payment information (such as credit card numbers) must always be ensured for transmission thereof; - Applicable customer information requirements as per *s@fer-shopping*™ are complied with.
UBE (Independent Booking Engine) Tool for research and booking on the basis of an independent third-party agent's terms and conditions of business (e.g. holiday homes)	- Clear identification as "external"; - Identification of the partner by the provider - Data protection and security must be adequately considered in partner selection;. - Not included in *s@fer-shopping*™ certification.
INFO-P (Information Tool for Compulsory Information) Provision of information as per the information duties of tour operators (e.g. conditions of entry into a country).	- Clear identification as "external" - Identification of the partner by the provider - Complete and up-to-date information - Easy to research. - Information easy to print out.
INFO-F (Information Tool for Optional/Voluntary Information) Provision of additional information (e.g. weather).	- Clear identification as "external". - Identification of type of offering. - Not included in *s@fer-shopping*™ certification..

The organization ordering *s@fer-shopping*™ certification must take steps to obtain any approvals necessary for partial assessment of partners.

Annex 2: Disclaimer

TÜV SÜD Management Service GmbH (TSMS) has developed requirement catalogs outlining the prerequisites for awarding the certification mark to online merchants.

Within the core competencies of TSMS, these requirement catalogs define the technical and ergonomic requirements and requirements pertaining to the organizational structure of online sales that must be satisfied prior to awarding the *s@fer-shopping*™ mark. The *s@fer-shopping*™ certification mark will only be awarded to online merchants after the latter have been thoroughly assessed for compliance with these requirements. Nevertheless, TSMS cannot guarantee that all underlying quality and security requirements are always satisfied by online merchants.

Technical and ergonomic requirements must largely be oriented to the statutory provisions and requirements. For this reason, the requirement catalog also includes criteria in correspondence to the text of the relevant law. The award of the *s@fer-shopping*™ certification mark to online merchants does not replace legal, tax-law or business consultancy.

Assessment of Internet offerings for compliance with the requirement catalog prepared by TSMS does not include any legal review within the meaning of the Legal Counseling Act. Above all, it does not include review of adherence to statutory provisions in as far as the latter exceed technical and ergonomic requirements and the comprehension of users, especially that of customers/purchasers.

TSMS expressly points out that a contract to assess an Internet offering does not involve a contract for legal counseling services at the same time; customized legal recommendations or legal information are not provided.

TÜV SÜD Management Service GmbH
Internet-Zertifizierungen s@fer-shopping
Ridlerstrasse 65
D-80339 München

Tel.: 089 / 57 91 - 43 00
Fax: 089 / 51 55 - 10 97
e-Mail: info@safer-shopping.de
Internet: www.safer-shopping.de