Sec-IT

Choose certainty.
Add value.

Requirements catalogue for the assessment and certification of online contract conclusion

version 5.1
dated 2019-09-19

Note: This requirements catalogue can be applied to various forms of online contract conclusion (e.g. purchasing goods, services, booking travel, buying insurance).
The certification focuses on the online sales channel. Evaluating the (insurance) products is not the subject matter of the assessment.

Contents

Sec-IT

1 Organizational requirements

1.1 Responsibilities and authorities have been clearly and completely defined in order to ensure satisfaction of all requirements from this catalogue as well as relevant statutory regulations. Suitable arrangements have been made regarding substitution.

1.2 Procedures suitable for implementing the requirements have been established.

1.3 The organization determines and assesses customer requirements as well as customer satisfaction at regular intervals. The results of the evaluation of customer satisfaction are used for continuous improvement.

2 Data security

2.1 A suitable security concept has been established to ensure appropriate protection of the contents of the internet offering and the personal data of users and customers. The provider addresses possible threats and resulting risks. Appropriate security measures are defined on this basis.

2.2 The security measures in the security concept adequately counteract all relevant threats. For this purpose and to an appropriate extent, the provider also takes the following measures:

- Systems and applications have been professionally installed and their security standard is kept up to date.
- Personal data may only be accessed by appropriately authenticated persons.
- Relevant data is backed up on a regular basis.
- Encryption technology conforming to generally accepted codes of practice is applied to ensure the protection of privacy, payment information or other sensitive data protection.

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

3 Data protection

3.1 The responsibility for data protection has been assigned within the organization. Depending on pertinent laws and regulations a data protection official might have to be appointed.

3.2 An inventory of all relevant processing activities pertaining to personal data exists.

3.3 Employees in contact with personal data have been trained with regard to relevant data protection regulations.

3.4 If personal data is transmitted to a third party or made accessible in any way to a third party, an agreement shall be obtained which ensures that the third party employs appropriate measures to protect this data. The same applies if personal data is processed on behalf of the data controller or if access to personal data cannot be ruled out.

3.5 Without the user's consent, personal data may only be processed in as far as this is required for establishing, shaping or amending a contractual relationship or it is legally permitted (e.g. the processing can be legitimized on the grounds of a corresponding weighing of the legitimate interests of the data controller against those of the data subjects).

3.6 Declarations of consent may be effected electronically via unambiguous, informed, voluntary and deliberate acts on the part of the user (e.g. by activating an appropriately labelled checkbox).

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

3.8 Users will be informed about the type, scope and purpose of the processing of personal data, unless such information has already been provided. It must be possible to call up this information at any time. In particular, the data controller is clearly identifiable and a possibility for making enquiries regarding data protection is provided.

3.9 If users are to be contacted for consulting, advertising or market-research purposes or to shape communication and information services in line with demand, they shall be informed beforehand with regard to the respective purpose and their right to object to this at any time. This information can be accessed at any time.

3.10 Electronic promotional communication (e.g. newsletter via e-mail) with a customer or interested party is only permissible if the user has expressly declared consent therewith. Exceptions to this consent are only permissible in due consideration of laws and regulations against unfair competition pertaining to unconscionable pestering or other statutory regulations.

3.11 Each promotional communication shall provide the user with the possibility of immediately withdrawing his or her consent (e.g. via an internet address).

3.12 Suitable procedures are defined to ensure correct handling of data subjects‘ rights.

Sec-IT

4 Online contents and processes

4.1 Range of offers and contents

a) Only offerings and contents complying with the statutory regulations are provided. In particular, provisions regarding the protection of minors must be observed.

b) An online shop offering foodstuffs via the internet must be able to provide TÜV SÜD with evidence of its official registration as a food business operator.

4.2 General information

a) The following general information will be made available to users: Full name and identity of the online merchant as well as address, email address and telephone number (no premium rate number). This information is easily found and directly accessible at a conspicuous location.

b) If restrictions exist with regards to shipment destinations, this is made clear at the beginning of the checkout process at the latest.

c) General Terms and Conditions of Business (GTC) – if any – are easily accessible.

4.3 Details regarding goods / services as well as costs and other customer information

To enable users to obtain a comprehensive picture of the goods and services and the associated costs, the following information will be provided:

a) Information prior to starting the process of placing an order / booking or applying for insurance:

- Essential features of the product/service, travel or insurance
- Price of the product/service, travel or the insurance premium including all taxes (unless only business to business transactions are concerned) and any other price components as well as – if applicable – the cost of shipping and handling and additional fees if any. It is obvious which components are included in the quoted prices and in which currency the prices are quoted. If prices are broken down, the total must be highlighted.
  In addition, for travel industry websites (e.g., online travel agencies, -tour operators‘ booking websites): The price must include the booking fee, but not the cost of travel insurance, variable costs for energy and cleaning or visitor’s taxes. Air fares are to be quoted including airport charges and taxes.
- Payment details, including information about methods of payment and the provider's special terms and conditions of payment (e.g., special fees for certain payment procedures).
- Details regarding delivery or fulfilment (in particular the estimated delivery date).

Specifically, for online shops (e.g., selling goods, services) and for online insurance:

- Minimum duration of contract, if the contractual contents involve a permanent or regular service, as well as information on ways of terminating contracts which involve a continuing obligation and are valid for more than one year or indefinitely.
- If applicable, provision of the right of cancellation and possible exclusions of the right of revocation (see Article 4.8).

Specifically, for travel industry websites (e.g., online travel agencies, tour operators‘ booking websites):

- Information on ways of terminating contracts and notice periods in this context.

b) At the latest on delivery of the products or on rendering of services, information according to Articles 4.2 a) and 4.3 a) as well as General Terms and Conditions of Business, if any, (unless only business to business transactions are concerned) will be made available to the customer in text form.

4.4 Research, selection and placing an order / booking travel / applying for insurance

The functions for researching, selecting and ordering products and services or booking travel or applying for insurance are correct, transparent and easily usable.

a) All relevant information (e.g., about providers, services, terms and conditions of business, data protection) can be accessed easily. They are easy to understand and meaningfully presented in context.

b) Queries regarding offerings and services are executed correctly; contents are logical and consistent.

c) When entering information, users can clearly recognize which entries are mandatory and which entries are optional. Only personal data necessary for fulfilling the contract is collected mandatorily.

d) Errors made when entering information can be recognized and corrected.

e) Users are well aware in advance of precisely when they will place an order / make a booking and a contract will be concluded or an application for insurance is made. In this context, the fact that they are now about to place an order / make a booking or apply for insurance, and that their next click will be binding is clear to users.

f) Users can cancel the process of ordering / booking or applying for insurance at any time without having placed an order / made a booking or applied for insurance.

g) Receipt of the order / booking or insurance application is confirmed electronically to the customer without delay. In particular the following information is included: all products that have been ordered or all services that have been booked / applied for and their prices, the specific costs of shipping and handling, if any, all other additional costs, the total price, and, if applicable, the estimated delivery date.

h1) For online shops (e.g., selling goods, services):

- A summary of the goods and services selected by the user as well as their prices can be accessed by the user at any time.
- Products can be “put back” individually before ordering.
- Before ordering, all selected goods and services are summarised with individual and total prices.

h2) For travel industry websites (e.g., online travel agencies, tour operators‘ booking websites):

- Before booking, all selected services are summarised and the travel price is quoted.
- After the booking, the customer receives – if applicable – evidence of insolvency insurance in the form of a security document according to Art. 651 k of the German Civil Code (BGB).

h3) For online insurance:

- Before applying for insurance, all selected services are summarised and the insurance premium is quoted.

4.5 Payment process

Basic payment functions are correct, transparent and easily usable.

a) An overview of available payment methods can be easily obtained.

b) Details of the payment process are easy to understand and meaningfully presented in context.

c) At least one payment method that is free of charge and well-established is offered to customers.

d) Customers receive a payment confirmation that is clearly assignable to the order / the booking or the insurance contract (e.g.. clear identification on the bank statement).

e) If credit card transactions are carried out, the requirements of the Payment Card Industry Data Security Standard (PCI DSS) must be adhered to.

Sec-IT

4.6 Delivery

a) The organization has established an effective process to ensure timely and complete delivery of all products ordered, or of all travel documents within an appropriate time frame prior to travel and – if applicable – within the deadline defined to the customer, or to ensure processing of insurance applications and delivery of insurance documents within the deadline defined to the customer or, if no deadline has been defined, within an appropriate time frame.

b) The client shall be informed immediately if the agreed delivery time cannot be honoured.

c) Additionally, for travel industry websites (e.g., online travel agencies, tour operators' booking websites): In case that a tour has to be cancelled, the customer is to be informed about this and about available options in due time.

4.7 Customer service

The online merchant offers appropriate customer service (e.g., assistance in using the website, details regarding goods and services, handling of orders/bookings and complaints).

a) Customers can contact the online merchant. In addition to an email address, customers should also be provided with a telephone number to enable rapid contact at a reasonable rate.

b) Customer queries and complaints are properly answered within a reasonable period of time.

c) Client communication via email contains the full name and identity of the online merchant.

4.8 Right of cancellation (if applicable)

In particular, not applicable for travel industry websites.

a) Customers are granted the right to cancel the contract for a minimum period of 14 days, unless legal provisions stipulate other time limits or allow for exceptions from the right of cancellation.

b) The right of cancellation must not be unduly restricted.

c) In the case of a cancellation all payments made shall be reimbursed within 14 days unless legal provisions stipulate other time limits.

d) There are rules as to who incurs the cost of return shipments. The customer is informed accordingly in due time.

4.9 External partners

Online merchants may cooperate with a number of partners in front-end transactions in the form of integrated external content. The following requirements apply to such content, if a tool for researching and ordering/booking on the basis of an independent third party's conditions of business is concerned (inclusion of external services, e.g., online photo service, flower dispatch, travel services):

- clear identification as "external"
- Full identification of the partner and the partner's privacy policy are available.
- Data protection and data security must be adequately considered in partner selection.
- Transmission of payment information (such as credit card numbers) must generally be secured adequately (accepted codes of practice).
- not subject of *s@fer-shopping* certification

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

Sec-IT

Annex: Disclaimer

TÜV SÜD Sec-IT GmbH (Sec-IT) has developed requirement catalogues outlining the prerequisites for awarding the certification mark to online merchants.

Within the core competencies of Sec-IT, these requirement catalogues define the technical and ergonomic requirements and requirements pertaining to the organizational structure of distance selling 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, Sec-IT 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 catalogue 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 catalogue prepared by Sec-IT does not include any legal review within the meaning of the Legal Counselling 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.

Sec-IT expressly points out that a contract to assess an internet offering does not involve a contract for legal counselling services at the same time; customized legal recommendations or legal information are not provided.