TÜVNORD

DESCRIPTION OF THE CERTIFICATION PROCESS
Trusted Site Data Privacy (TSDP)

TABLE OF CONTENTS

Do you have any questions about the service description? We are happy to help.

Website on data protection certification in accordance with Art. 42 GDPR:
Data protection certification in accordance with Art. 42 GDPR

TÜV NORD CERT GmbH
Business Entity IT
Am TÜV 1
45307 Essen
www.tuev-nord-cert.de

1. PURPOSE

Data protection certification in accordance with Art. 42(1) GDPR is a procedure that can be used to check processing operations for IT products, services or within a company with regard to compliance with legal data protection requirements.
The result is a data protection certificate that proves the implementation of the data protection standards of the GDPR.
The framework for certification is provided by Art. 42 GDPR, with which the EU promotes the introduction of data protection-specific certification procedures and the awarding of data protection seals and marks by certified bodies.
GDPR certification is generally aimed at all companies in which personal data is processed and/or stored using IT-supported processing procedures.

2. SUBJECT OF EVALUATION

The subject of evaluation is the specific object of an evaluation. The subject of evaluation is data processing by information processing services (IPS). IPS can only be processing operations in accordance with Art. 42(1) GDPR. Both software and combined software/hardware solutions can be used to provide IPS.
In addition to the IPS itself, the following criteria also consider its operational concept. This is seen as an intrinsic part of the IPS, as it describes important requirements for the data protection-compliant handling of the technical components of the IPS. Accordingly, the documentation of the IPS and its application specifications plays an essential role in the assessment.
Overall, the following components of the IPS are part of the evaluation:

A The IPS in its technical form as combinations of
- A1 hardware-,
- A2 software-, and
- A3 network components, as well as
- A4 Processes supported by these components

B The documentation of the IPS with the description:
- B1 Properties of the IPS (process documentation, technical/specialised),
- B2 Instructions for use of the IPS (technical/functional user documentation),
- B3 Separate operational concept /operating concept, if applicable (unless included in B1/B2),
- B4 Change information.

C Documents and other information provided for use with the IPS:
- C1 Forms,
- C2 Information texts (e.g. consent texts),
- C3 Websites,
- C4 Contract texts (e.g. contract for order processing).

To determine the object of the evaluation, the applicant must carry out a complete data flow analysis of the IPS, taking into account all actors involved in the processing of personal data, e.g. processors, sub-processors, joint controllers, and then prepare and submit a qualified representation of the entire processing process organised by phase, including a description of the respective actor and role model (actors, roles, relationships) for each processing phase.

The representation can either be a graphical representation (e.g. using standardised representations such as Business Process Modelling (BPM) or Unified Modelling Language (UML)) or in text form.
The qualified representation of the processing process must depict the complete life cycle of the processing of personal data within the IPS.
The definition of "processing" in Art. 4(2) GDPR does not provide an exhaustive list of individual processing operations.
In addition, it must be determined and documented which data processing steps are to be assigned to the applicant's extended area of responsibility. In this context, it must also be clearly stated how the access options of the controllers and processors are structured in the respective data processes. All data processing steps and relevant interfaces must be recorded in full. The applicant must also identify the processing operations to be certified, which are the subject of the evaluation, so that the respective evaluation object can then be determined in consultation with the certification body and considering the information provided in 1.7 to 1.17 of the criteria catalogue [D503-10VA02A01_Criteria Catalogue TSDP_2.12], the respective evaluation subject can be determined.
The applicant must provide detailed information in accordance with 1.7 to 1.17 of the criteria catalogue [D503-10VA02A01_Criteria Catalogue TSDP_2.12] in order to define the subject of the evaluation before the evaluation process begins. Based on this information, the subject of evaluation is then determined and documented accordingly in the Trusted Site Data Privacy evaluation report [D503-10VA02F002_ Evaluationreport_Template_TSDP].

3. OVERVIEW OF THE CERTIFICATION PROCESS

The requirements are checked using the TN CERT "Trusted Site Data Privacy" criteria catalogue.
The various phases of the certification process are described in the following sections.

3.1. Request for quotation and certification agreement

The customer for certification sends his enquiry about the certification process to the certification body. The certification body provides information about the certification process, and the customer receives the following documents on request:

- "Data protection certification enquiry form in accordance with Article 42 GDPR - Trusted Site Data Privacy"
- a „Kickoff“ (workshop) offer,
- a certification offer,
- the certification agreement form with the certification conditions,
- description of the certification process.

The customer provides a description of the certification object (scope) for the preparation of the offer. For this purpose, the customer must complete the "Data protection certification enquiry form in accordance with Article 42 GDPR - Trusted Site Data Privacy" [D503-10F100]. If necessary, questions regarding the definition of the scope of certification or the certification procedure will be clarified in a preliminary meeting. It is then checked whether the desired evaluation object is generally certifiable.

An offer is then made for a "kick-off" workshop. This may not be necessary, e.g. in the case of re-certification, as the subject of certification is already known. As part of the "kick-off" offer/workshop, the certification procedure and (by the customer) the respective object of evaluation are presented. The aim is to gain a common understanding, clarify all questions and determine the specific scope of the certification. If it turns out in this step that the desired object of evaluation cannot be certified, the process ends at this point. In the positive case, the costs are finally calculated, and a certification offer is prepared.
The customer then places the certification order based on the certification body's certification offer and accepts the certification conditions by signing the certification agreement form. The application is then accepted, and the order is confirmed with notification from the responsible evaluation manager.

3.2. Preparation for the evaluation

The evaluation is carried out by an evaluation team under the responsibility of the evaluation manager in accordance with the requirements and specifications of the certification body. The evaluation team plans the schedule for the evaluation with the customer and, if necessary, clarifies any remaining uncertainties regarding the evaluation and certification process in preliminary discussions.
The evaluation comprises all activities to obtain complete information on the fulfilment of the specified requirements by the subject of certification. This includes planning and preparatory activities. The evaluation is based on the TSDP criteria catalogue completed by the customer with any additional documents.
The language for the evaluation and the evaluation documentation is agreed with the customer prior to the evaluation. German or English language/writing is offered.
The evaluation manager makes the final decision as to which elements of the evaluation object and which organisational activities are to be evaluated within a specified time frame and which technical tests are to be carried out within a specified time frame. The customer is informed of the scope of the evaluation by the evaluation manager.
The evaluation is carried out using various evaluation methods. These are described in detail in the TSDP criteria catalogue.

3.3. Evaluation

The evaluation is carried out by evaluators who are employees of the certification body or are approved by the certification body and who meet the competence requirements of the abovementioned document in its currently valid version.
The evaluators examine the processing operations to be certified with regard to conformity with the above-mentioned relevant standards. As part of the evaluation, it is determined whether the applicant's processing operations comply with the European legal requirements of the GDPR and whether the applicant has taken the technical and organisational measures required of it in order to ensure the permanent conformity of its own actions with the requirements of the GDPR.
The evaluation of the processing operations is divided into three phases:

- documentation review
- technical evaluation activities
- evaluation.

When assessing the test criteria, a distinction must be made between "Fulfilled", "Fulfilled with recommendation" and "Not fulfilled". "Fulfilled with recommendation" certifies conformity but indicates a suggestion for improvement that the customer should have analysed by the next surveillance or recertification.
"Not fulfilled" defines non-conformity, which results in the certificate not being issued or, in the case of an existing certificate, being suspended.
Conformities must be established within a specified period set by the evaluator, which may not exceed 6 months, otherwise the certificate will definitely not be issued or will be permanently withdrawn.

3.4. Evaluation report

Once the evaluation has been completed, the evaluators draw up an evaluation report based on the results of the document review and technical evaluation. This report is made available to the customer and forms the basis for the assessment and certification decision.

3.5. Granting of certificates

The certification body assesses the evaluation on the basis of the evaluation report prepared, the evidence collected and the verification of compliance with the certification body's procedural requirements.
After approval, the evaluation report is made available to the customer as a draft.
In the event of a negative certification decision, the customer is informed in writing of the reasons for the decision. The customer is granted a period of 4 weeks to appeal against this decision in writing.
In the event of a positive certification decision, the certificate is issued with a maximum validity period of three years.
The certificate is sent to the customer for approval before it is issued. At least two inspections must be carried out during the three-year period of validity of the certification.
To support the transparency of certifications, the certification body maintains a list of certified products, which is made available to the public.
New certificates are published on the website following a positive certification decision.

4. CERTIFICATE VALIDITY AND MONITORING

Within the certificate term (3 years), the certification body carries out unannounced monitoring audits. These should take place annually within the last six months of the past year in order to maintain the validity of the certificate.
The monitoring schedule is based on the certificate date. Monitoring must always be completed at the latest on the day one or two years after the certificate date. The earliest start date for surveillance is six months before this date. Recertification may also begin no earlier than six months before the end of the certificate term. A maximum of two surveillance periods are possible. A complete evaluation is required after 3 years at the latest in order to extend the validity of the certificate.
As part of the monitoring process, the activities are carried out as for the initial certification in accordance with this document. In terms of content, it is determined whether the facts set out in the certification continue to apply or whether changes are compliant with the certification. In addition, updated or new standards are taken into account where applicable. The review can be based on a representative sample.

If non-conformities are identified during the monitoring, a plan to rectify these non-conformities must be agreed with the customer within a set period. As a rule, this deadline should not exceed 3 months after the non-conformity is announced in the evaluation report. If the complexity of the planned corrective action so requires, the deadline can be extended to up to 6 months after the non-conformity is announced in the evaluation report.
The customer must ensure that its processes are processed in compliance with data protection regulations during the term of the certificate. In the event of anomalies that give rise to concerns about non-compliance with the certification requirements, event-related monitoring shall be carried out.

5. CHANGES IN CERTIFICATION

In the event of changes in factual or legal circumstances that are capable of altering the conformity assessment of the test object after the certificate has already been issued as part of a certification or recertification, the certification body or the customer is obliged to inform the other party immediately of the occurrence of the respective circumstances. If the occurrence of such a circumstance can already be predicted with certainty (e.g. the passing of a law that will come into force on a specific date; planned change to an internal operational process), both parties are obliged to inform the other party in writing of the circumstance within three months.
In this case, the certification body decides which measures are necessary in order to maintain the certification in view of the changes. As a result of this decision, a re-evaluation, assessment, decision or preparation of revised formal certification documentation may be deemed necessary. In addition, the head of the certification department may also decide to extend or restrict the scope of the certification.
If maintenance of the certificate requires the implementation of certain measures, these must be implemented by the customer within three months.
If maintaining the certificate requires the implementation of certain measures, these must be implemented by the customer within three months.
Changes to the certification initiated by the customer include:

- significant changes to the TSDP documentation,
- safety-related changes.

A complete reassessment of the evaluation object shall be carried out in the event of

- significant changes to the scope,
- significant changes in the services provided within the scope,
- the inclusion of new services in the scope,
- significant changes to the IT systems or business processes of the TSDP and/or
- if a significant part of the services is relocated to another location.

The certification body shall decide on the basis of the description whether a new document review or a new technical evaluation is necessary or whether the changes can be reviewed as part of the next surveillance or recertification evaluation. In the event of a new document review or evaluation, the evaluators shall prepare a corresponding evaluation report, which shall be made available to the customer.

If non-conformities are identified during the review of changes, a plan to rectify these non-conformities must be agreed with the customer within a set period. As a rule, this deadline should not exceed 3 months after the non-conformity is announced in the evaluation report. If the complexity of the planned corrective action requires it, the deadline can be extended to up to 6 months after the non-conformity is announced in the evaluation report.
After each change, the certification decision is made as to whether an updated certificate can be issued with the changes.