Rules of Procedure for Certification According to the Trusted Cloud Data Protection Profile for Cloud Services (TCDP)

Prodecure for certification under the

Contents

Rules of Procedure for Certification According to the Trusted Cloud Data Protection Profile for Cloud Services (TCDP)

Preamble

Certification according to the Trusted Cloud Data Protection Profile for Cloud Services (TCDP) is available for all cloud services within the scope of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, (BDSG)). TCDP is an standard for the certification of the data protection compliance of cloud computing services that has been developed on behalf of the Federal Ministry for Economic Affairs and Energy (BMWi) as part of the "Data Protection Certification for Cloud Services" pilot project (hereinafter referred to as "pilot project").

The purpose of the TDCP certification is on one hand to enable domestic and foreign providers of cloud services, and their subcontractors, to demonstrate compliance with the requirements of the Federal Data Protection Act and on the other hand to provide users with a reliable tool to rely on the cloud providers' compliance.

The TCDP certification procedure has not been specifically regulated by law up to now. A TCDP certificate may only be issued under the conditions set down in the following Rules of Procedure.

Chapter 1: Scope

§ 1.1 Scope

(1) These Rules of Procedure apply to the certification and audit of cloud services under TCDP.
(2) TCDP certification is open to all cloud services that fall under the Federal Data Protection Act or that are bound by contract with the cloud user or contractor to comply with the requirements of the Federal Data Protection Act.

§ 1.2 Subject of the certification and audit

(1) These Rules of Procedure apply to all cloud service providers as defined by the National Institute of Standards and Technology (NIST), i.e. services that are characterized by (1.) on-demand self-service, (2.) broad network access, (3.) provider-

side resource pooling, (4.) rapid elasticity and (5.) measured service, and can be classified as an Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) that are provided for a user of such services (cloud user). For the purposes of these Rules of Procedure, cloud services include component services making up the cloud service and services that the cloud service provider uses to provide his cloud service and that have access to personal data in this context.

(2) Cloud service providers are legal entities that offer cloud services.

§ 1.3 Relation to DIN EN ISO/IEC 17065

(1) These Rules of Procedure constitute a certification programme within the meaning of DIN EN ISO/IEC 17065.

(2) Cloud services are services within the meaning of DIN EN ISO/IEC 17065.

Chapter 2: Certification body and audit body

§ 2.1 Certification body

(1) Certification according to TCDP shall be performed by an independent certification body with appropriate expertise. The certification body shall be non-discriminatory and impartial in the performance of its duties.

(2) The certification body can be an organisation having legal capacity or a separate part of an organisation having legal capacity.

(3) The certification body must have the necessary financial stability and resources to perform the service.

(4) The certification body shall guarantee the confidentiality of information concerning and deriving from the certification procedures.

§ 2.2 Certifiers

(1) Certifiers are natural persons who are responsible for the performance of the certification process on behalf of a certification body. The certification process can be performed by several certifiers working as a team In this case it is sufficient if the professional requirements as set down under (2)-(4) are met by the team as a whole. The personal requirements defined under (6) and (7) must be met by each individual within the team.

(2) Certifiers must demonstrate sufficient competence and suitability for the assessments they perform.

(3) Certifiers must have a university degree or training to an equivalent standard.

(4) A certifier must have sufficient knowledge in the fields relevant to the certification. In particular, a certifier must have sufficient knowledge in the following fields:

a) Data protection requirements for cloud services under the Federal Data Protection Act;
b) Technical principles of cloud services;
c) Technical requirements for data security;
d) ISO/IEC 27000 seriries of standards;
e) TCDP certification procedure and standards.

(5) Sufficient experience for certification requires at least four years working full-time in the field of information technology or data protection and at least two years working full-time as a certifier or at least four years of experience working full-time as an examiner of products and/or services in the field of data protection or information security.

(6) On the basis of their character, conduct and skills, auditors must demonstrate the level of ability required to perform their tasks properly. Certifiers must be independent as defined in Section 2.7 (3). They shall be non-discriminatory and impartial in the performance of their work.

(7) The certification body shall ensure that the certifiers they engage meet the requirements set down in (2) to (7).

§ 2.3 Audit body

(1) Audit bodies or individual auditors with appropriate expertise can be appointed to audit a cloud service for the purpose of TCDP certification. If an individual auditor is appointed, the requirements governing assessment organizations apply accordingly for the auditor.

(2) An audit body is a legal entity or part of an organisation with legal capacity that engages auditors to perform audits according to these Rules of Procedure.

(3) The audit body shall be non-discriminatory and impartial in the performance of its work as defined in Section 2.7 (1) and (2) and shall have the necessary resources to perform the audit.

(4) The audit body shall guarantee the confidentiality of information concerning and deriving from the audit procedures.

(5) The audit body can appoint its own auditors or external audotors to perform the audit.

(6) The audit body must take out and maintain appropriate liability insurance.

§ 2.4 Auditors

(1) Auditors are natural persons who perform audits according to these Rules of Procedure for an audit body or because they are contracted to do so by the cloud provider.

(2) Auditors must demonstrate sufficient competence and suitability for the audits they perform. This requires adequate education and experience.

(3) Auditors must have a university degree or equivalent training in the fields relevant to the audit. Within this context, legal training is required with regard to the legal

TCDP requirements and technical training is required with regard to the technical TCDP requirements.

(4) In particular, auditors must have sufficient knowledge in the following fields:
   a) Data protection law requirements for cloud services;
   b) Technical principles of cloud services;
   c) Technical requirements for data security;
   d) ISO/IEC 27000 seriries of standards;
   e) TCDP certification procedure and standards

   With regard to points (a) to (d) above, it is sufficient for the legal auditor to have basic knowledge concerning (b), (c) and (d) and for the technical auditor to have basic knowledge concerning (a).

(5) Sufficient experience for the audit requires at least four years of experience working full-time in the field of information technology or data protection and at least two years of experience working full-time in the area of evaluating IT products and IT procedures in the field of data protection or information security. Work as a data protection officer or an IT security officer or as a consultant in the aforementioned fields does not constitute work experience within the meaning of the requirements under this section 2.4 (5).

(6) In addition, auditors must have the necessary personal eligibility and reliability integrity to perform the audit.

(7) Auditors must be independent within the meaning of Section 2.7 (3) and be non-discriminatory and impartial in the performance of their work. They may not be involved in the audit of a cloud service if this could be a source of a conflict of interest within the meaning of Art. 2.7 (4).

§ 2.5 Accreditation

(1) The certification body and assessment organization must have an accreditation to demonstrate their compliance with the requirements of these Rules of Procedure, and particularly their professional competence and suitability.

(2) Certification bodies need accreditation by the German national accreditation body, DAkkS, for certification according to these Rules of Procedure.

(3) If the DAkkS does not have a specific accreditation procedure for certification bodies according to TCDP, the following accreditations shall be construed as accreditation for certification bodies for the purpose of these Rules of Procedure:
   a) DAkkS accreditation according to ISO/IEC 17065 for the area of IT security (ISO/IEC 15408, ETSI EN 319 401);
   b) DAkkS accreditation according to ISO/IEC 17021 for information security management systems according to ISO/IEC 27001.

(4) The certification body may only perform certifications according to these Rules of Procedure if they have valid accreditation.

(5) Assessment organizations need DAkkS accreditation for assessments according to these Rules of Procedure.

(6) If the DAkkS does not have a specific accreditation procedure for assessment organizations according to TCDP, the following accreditations shall be construed as accreditation for assessment organizations for the purposes of these Rules of Procedure:
    a) DAkkS accreditation according to ISO/IEC 17025 for the area of IT security (ISO/IEC 15408);
    b) Admission as an expert body pursuant to Section 9 (3) of the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, (BSIG));
    c) Admission as an assessment organization or expert for the data protection quality label from ULD Kiel, the Independent Centre for Privacy Protection;
    d) Licence as an expert for the preparation of expert reports in the certification procedure defined by European Privacy Seal GmbH (EuroPriSe).

(7) The professional competence and suitability of the audit body and the certification body only applies for the time and scope defined in the accreditation. The accreditation of the audit body and the certification body must also be valid at the time the audit and certification procedure are concluded.

§ 2.6 Relationship between the certification body and the audit body

(1) The certification body and the audit body can belong to the same organisation. In this case, neither the certifier nor the auditor case have authority over the other.

(2) The certification body can define a procedure for the approval of audit bodies. In this case, the approval must be according to transparent, non-discriminatory and objective standards. The certification body must keep a list of the audit bodies it has approved and must make this list available to the public at all times.

(3) If the certification body performs an approval procedure as defined in (2), it can specify that it will only accept certification assignments if the audit is performed by an audit body it has approved.

§ 2.7 Independence and impartiality. Risk of a conflict of interest.

(1) Certification bodies and audit bodies, certifiers and auditors are considered independent if they are free from external and internal influences, particularly of a financial nature.

(2) Certification bodies, audit bodies, certifiers and auditors are considered impartial if they perform their certification and audit work objectively as set down in these Rules of Procedure and are not guided by extraneous interests, particularly economic or personal interests.

(3) Certification bodies and and audit bodies shall take suitable organisational measures to guarantee the independence and impartiality of the certifiers and auditors. They shall contractually obligate the certifiers and auditors to maintain their independence. Due consideration must be given to the following principles, in particular, when meeting the requirements of this sub section 2. 7 (3):

a) Any form of influence by other parties or organisations on the audit and the audit results is forbidden.
b) The certifier's and auditor's remuneration are not contingent upon the results of the assessment or audit, nor on the number of assessments or audit performed.
c) Certification and audit activities may not be combined with other tasks which, depending on the type or intensity of the task in question, could result in a conflict of interest and therefore negatively impact the quality of the certification or audit work.
d) At the time of certification or audit, neither the appointed certifier and auditor, nor other members of staff directly or indirectly involved in the certification or audit activity, may have a relationship with the cloud service provider that goes beyond the audit assignment.
e) The certifiers and auditors may not provide consultancy services, or other services which could jeopardise the independence of the certification/audit, for the cloud service provider in the period two years prior to the certification or audit and two years after the certification.

(4) Certification bodies, certifiers, audit bodies and may not perform their services if there is a risk of a conflict of interest. This risk particularly arises if certification bodies, certifiers, audit bodies and auditors design, implement or offer cloud services or components of cloud services, or advise providers of cloud services or components of cloud services, in the period two years prior to the audit or certification process, or during the audit or certification process, or agree to perform such an activity with a provider of cloud services in the future.

§ 2.8 Compensation

The certification body and audit body are entitled do appropriate compensation for their work. The compensation must be set forth in the contract with the cloud service provider.

Chapter 3: The audit procedure

§ 3.1 Contractual basis

(1) The audit procedure is based on a contract between the cloud service provider and the audit body.
(2) The contract shall specify the following at least:
a) The scope of the audit with information related to all the locations relevant for the operation of the cloud service;
b) The version of the TCDP requirements in force at the time;
c) These Rules of Procedure as the definitive procedural arrangement for audit and certification;

d) The audit assignment (scope and place of the audit, scheduled duration, audit report) including the protection requirement category requested by the cloud service provider;
e) The certification body that will perform the certification;
f) Obligations of the cloud service provider to co-operate.

When describing the scope of the audit, applicants must specifically indicate which components form part of the cloud service.

§ 3.2 Obligations of the cloud service provider to co-operate

(1) The cloud service provider shall, at its own expense, take all necessary measures which are required for the correct audit and certification including all measures but not limited to all measures contractually agreed.
(2) In particular, the cloud service provider is required to supply the audit body with sufficient documentation concerning the scope of the audit or grant the audit body access to this information. In addition to a description of the cloud service, the documentation shall include, in particular, the technical and organisational measures of the cloud service provider as defined in Section 9 of the Federal Data Protection Law (*Bundesdatenschutzgesetz*, (BDSG)).
(3) The cloud service provider shall assure the audit bodythat the measures cited in the documentation are fully implemented.
(4) If the cloud service provider seeks recognition of certificates for parts of its cloud service, it must communicate the request for recognition before the audit commences, specifying exactly the certificates to be recognized the part of the cloud service for which recognition is sought, and provide the documents which are relevant to assessing whether the certificate can be recognized.

§ 3.3 Audit procedure

(1) The audit shall be performed on the basis of the description of the scope of the audit as clearly defined in the agreement and at least consist of an examination of the documentation supplied by the cloud service provider (3), an interview (4) and an onsite inspection (5). Technical tests (6) must be performed where necessary.
(2) The interaction of the cloud service or component with other components or services shall also form part of the audit.
(3) With regard to the document examination, the auditor shall examine compliance with the requirements of TCDP on the basis of the information provided in the cloud service provider's documentation.
(4) The process of interviewing employees of the cloud service provider or other individuals who are involved in the delivery within the scope of the audit can be used to establish the facts concerning individual aspects of the audit and to verify the correctness of the documentation. The interview should be used, in particular, to aspects of the audit which the auditor considers critical. Interviews can be conducted in writing or in person. With regard to core subjects, they should be

conducted as an oral interview in any event. If a personal interview would be disproportionately expensive, the interview can be conducted in the form of video conferencing.

(5) The onsite inspection shall involve at minimum an inspection of the procedures and technical facilities at the premises of the cloud service provider or its subcontractors.

(6) Appropriate security-related tests shall be performed if required for the protection requirement category sought by the cloud service provider.

§ 3.4 Recognition of certificates

(1) If the certification body recognises existing certificates for components of cloud services, it is not necessary to eamine th component of the cloud service covered by the document. However, it is necessary to examine the interaction of a recognised component of the cloud service with other components, particularly the interfaces between those components.

(2) If the cloud service provider seeks recognition of existing certifcates, the audit body shall examine without undue delay whether and to what extent recognition is possible.

(3) The audit body can ask the certification body for a preliminary decision regarding the recognition of existing certificates. At minimum, the information and documents defined under Section 3.2 (4) must be enclosed with this request.

§ 3.5 Audit report

(1) The audit body shall draft an assessment report on the basis of the audit. The audit report shall contain the following information at minimum:

a) The scope of the audit;

b) An explanation of the scope and timeframe of the audit with information on the locations and premises where the audit was performed;

c) A brief outline of the implementation of the individual TCDP requirements;

d) A reasoned assessment of compliance or non-compliance with the individual TCDP requirements for the protection requirement category concerned;

e) The measures the audit body applied to determine compliance, particularly information on the examination method as defined in Section 3.3 (2) to (6) and - if necessary to aid understanding - reasons for the use of said measures;

f) Information on the certificates to be recognized and a statement concerning the examination of interaction of services;

g) Justification of the equivalence of certificates to be recognized as referred to in Section 4.5.

h) The overall result concerning compliance or non-compliance with TCDP requirements for a certain protection requirement category;

i) Justification for the overall result;
j) A list of the documentation which has been examined;
k) The declaration of the cloud service provider pursuant to Section 3.2 (3);
l) A statement concerning compliance with the individual ISO/IEC standards referenced by the TCDP. This statement can be in table format using bullet points or icons that indicate compliance or non-compliance with the individual ISO/IEC standard. The list can be supplied as an annex to the audit report;
m) The declaration of the auditor stating that the auditor has met the independence and impartiality requirements of these Rules of Procedure and that there is no reason to suspect a conflict of interest.

(2) The audit report can contain comments. The comments can also indicate whether TCDP requirements which have not yet been met could be satisfied and what actions the cloud service provider would need to take to do so.

(3) The scope of the audit must be identified precisely in the audit report. In particular, the function of the cloud service must be described and delimited in detail, and the technical facilities, including the premises relevant for the provision of the cloud service, must be described. Premises in which technical systems are operated and the workspace of individuals who control the cloud service are of significance.

(4) The scope of the auidit can be specified in an annex to the audit report.

(5) The audit body shall submit a draft of the audit report to the certification body for comment. The final version of the audit report may only be communicated to the cloud service provider once the certification body has provided its opinion.

(6) The audit body shall make the audit report available to the cloud service provider and grant the cloud service provider unrestricted rights of use. The cloud service provider may only make the auditreport available to third parties in full and specifying the date of issue of the report. The cloud service provider must impose appropriate limitations of use on said third parties. The audit body can reserve the right to publish and publicly reproduce as defined in Section 15 (2) of the Copyright Act (*Urhebergesetz*).

§ 3.6 Interim audit

(1) Interim audits can be performed at the request of the cloud service provider.

(2) On the basis of the interim audit, the certification body must determine whether the certified cloud service continues to satisfy the TCDP requirements according to the certified protection requirement category.

(3) The annual interim audit pursuant to Section 5.4 must be performed at the earliest at the end of the sixth month, and at the latest by the end of the twelfth month, after the date of issue of the certification, or after the times the interim audit was performed in subsequent years.

(4) The requirements for the audit shall apply accordingly for the interim audit. The scope of the interim audit must be such that the changes made to the cloud service since the last audit are evaluated. Suitable random checks must be performed to determine whether the cloud service on the whole continues to comply with the TCDP requirements.
(5) The cloud service provider shall be obligated to cooperate as set down in Section 3.2. In particular, the cloud service provider shall be required to document the changes to technical and organisational measures as defined in Section 3.2 (2).
(6) The audit body shall produce an interim auditt report and submit it to the certification body in good time before the interim auditt period expires. Section 3.5 applies accordingly.

Chapter 4: The certification procedure

§ 4.1 Contractual basis

(1) The certification procedure is based on a contract between the cloud service provider and the certification body.
(2) The contract shall specify the following at least:
    a) The cloud service to be certified (the scope of the certification), with information on all the locations relevant for the operation of the cloud service;
    b) The version of the TCDP requirements in force at the time;
    c) The audit body responsible for carrying out the audit;
    d) These Rules of Procedure as the definitive procedural arrangement for the certification;
    e) The certification assignment including information on the protection requirement category requested;
    f) Obligations of the cloud service provider to co-operate

§ 4.2 Prerequisites for certification

(1) To be awarded the certificate, the cloud service must be audited by an audit body in accordance with these Rules of Procedure. The cloud service provider must nominate the audit body and establish the selected body's accreditation Accreditation is assumed if the assessment organization is listed on a list maintained by the certification body as defined in Section 2.6.
(2) After concluding the contract, the certification body shall appoint a competent certifier for the cloud service provider and the audit.
(3) The audit body shall notify the certification body of the auditor whom it has tasked with the audit.
(4) The certifier shall coordinate the scope and duration of the audit and the audit schedule with the competent auditor and with the certification body and the cloud service provider. Any intended recognition of existing certificates also forms part of the coordination work.

(5) The certification body can reserve the right to take part in the on-site inspection either fully or in part. However, it may not perform any audit procedures or intervene in the audit process.

§ 4.3 Review of the audit

(1) The certification body shall review the audit report to determine whether the audit was performed correctly, particularly with regard to meeting the requirements of these Rules of Procedure, and whether the cloud service satisfies the TCDP requirements in the requested protection requirement category.
(2) The certification body can request the audit body to supply additional explanations or amendments to the test report.
(3) In consultation with the audit body, the certification body can obtain information and verifications from the cloud service provider if this is required for the certification decision.

§ 4.4 Recognition of TCDP certificates

(1) The certification body shall recognize existing TCDP certificates for components of cloud services with regard to their validity and protection requirement category if these certificates were issued in accordance with these Rules of Procedure.
(2) If recognized, the certificate can be issued for the entire period of validity as defined under Section 5.3. The certificate must be withdrawn if a recognized certificate expires. This does not apply if the component in question is recertified without undue delay and the certificate can be recognized, or if the component is immediately incorporated into the certificate for the cloud service as a result of change certification as defined under Section 4.9.
(3) The certification body shall monitor the validity of recognized certificates. It shall notify the cloud service provider in good time if recognized certificates are due to expire.

§ 4.5 ecognition of other certificates

(1) The certification body can recognize other certificates if they are equivalent to a TCDP certificate in terms of substance and procedure. It shall determine the protection category and the recoverability level with which the certificate is recognized.
(2) The other certificate is equivalent in terms of substance if it is based on requirements that are comparable with or exceed the TCDP requirements with regard to the protection level.
(3) The other certificate is equivalent in terms of procedure if it has been issued in a certification process that offers a guarantee that the audit and certification has been performed correctly which is comparable with the guarantee provided by these Rules of Procedure.

(4) The following certificates are considered to be equivalent in terms of substance and procedure:
– ISO 27001 certification on the basis of *IT Grundschutz*;
– Certificates according to SOC 2;
– Certificates according to the BSI Requirements Catalog for Cloud Computing.
(5) The certification body must give reasons for the acknowledgement, recognition particularly with regard to the protection category and the recoverability level.
(6) If a certificate is recognized, Section 4.4 (2-3) shall apply accordingly.

§ 4.6 Decision of the certification body

(1) The certification body shall decide whether to issue certification on the basis of the audit report, the certifier's assessment and other findings, where applicable.
(2) The certificate must be issued to the requested extent if the cloud service meets the corresponding TCDP requirements.
(3) The certificate can be issued with restrictions if the TCDP requirements are not met for the requested extent but the requirements of a lower certification level are met. In particular, the certificate can be issued for a shorter certification period or for a lower protection class.
(4) If a cloud service does not meet the TCDP requirements, the issuing of certification must be denied.
(5) Reasons must be given if the decision falls short of the application.
(6) The decision concerning the certification must be communicated to the cloud service provider. The decision must contain all the information concerning acknowledged recognized certificates and the information according to Section 4.5 (5).

§ 4.7 Revision

(1) The certification body can give the cloud service provider the opportunity to revise or modify the application for certification either before or after a decision has been made regarding the issuing of the certificate.
(2) The certificate must be issued accordingly if, as a result of the revision, the cloud service meets the TCDP requirements in line with the original or modified application for certification.

§ 4.8 Appeal

(1) The cloud service provider can lodge an appeal with the certification body against a decision adversely affecting the cloud service provider. Reasons for the appeal must be provided. The cloud service provider is adversely affected if the certification decision falls short of the application.
(2) The appeal must be submitted in writing (including email) within 4 weeks of receipt of the certification decision.
(3) The certification body shall examine whether there are grounds for appeal.

(4) If the appeal is directed against the audit or the findings of the audit body, the certification body shall notify the audit body that an appeal has been lodged and obtain a statement from the audit body.
(5) If the appeal is justified, the certification body shall change the certification decision. If the certification body rejects the appeal, the reasons for doing so must be stated.
(6) The decision concerning the appeal, and grounds for the decision, must be communicated to the cloud service provider in writing (including email)

§ 4.9 Change certification

(1) At the request of the cloud service provider, the certification body can change the certification statement via a change certification process if new certification would require a disproportionately high effort. In the event of a change, the certificate continues to exist with its original validity period.
(2) Change certification can be needed particularly if changes are made to the cloud service or if the TCDP is amended. The regulations for the certification procedure shall apply accordingly for the change certification process. Section 3.6 shall apply accordingly for the audit within the context of change certification.

Chapter 5: The certificate

§ 5.1 Issuing of the certificate and certificate content

(1) The certification body shall issue the cloud service provider a certificate in line with the certification decision.
(2) The certificate shall contain the following information:
    a) The cloud service provider, and abbreviated designation if necessary;
    b) The scope of the certification, and abbreviated designation if necessary;
    c) The certification body;
    d) The name of the applicable version of the TCDP, and abbreviated designation if necessary;
    e) The declaration stating that the certified cloud service satisfies the data protection requirements of the Federal Data Protection Act for contracted data processing in accordance with the TCDP in the applicable version for a specific protection category and a specific recoverability level (certification statement);
    f) A unique certificate number;
    g) The period of validity of the certificate;
    h) An annex containing the information according to Section 3;
    i) The TCDP certification mark.
(3) The annex to the certificate shall contain the following information:
    a) The clear and unambiguous name of the cloud service provider;
    b) The clear and unambiguous identification of the scope of the certification;

c) The designation of these Rules of Procedure as the decisive procedural framework;
d) The designation of the set of rules used by the certification body;
e) The clear and unambiguous name of the audit report and the audit body;
f) The exact designation of the applicable version of the TCDP;
g) The result of the audit.

(4) The certificate or the annex can contain the following additional elements:
a) Logo of the certification body;
b) The signature of an authorised representative of the certification body;
c) The description of the scope of the certification;
d) Comments from the certification body.

(5) If the sample certificate as defined in Annex 1) is used, the requirements under (2) and (3) are deemed to be observed.

(6) The certification body shall assign a unique certificate number to each certificate. This number shall consist of the clear and unambiguous name of the certification body, the word TCDP and a unique number within the certification body (e.g.: CERTIFICATION BODY-TCDP-0001).

§ 5.2 Certificate publication

The certification body shall keep a record of the certificates and publish the certificate and the annex on a publicly accessible website for the duration of the certificate's validity and for a further ten years. The certificates must be easily accessible.

§ 5.3 Period of validity. Recertification

(1) The certificate shall be issued for a maximum period of three years. The period commences with the date of issue indicated on the certificate.

(2) The cloud service provider can request to have the cloud service re-evaluated and re-certified according to these Rules of Procedure before or after the period of validity has elapsed.

(3) The rules of the (initial) audit and certification shall apply for the new audit and certification. The cloud service provider can contract the audit body that performed the previous audit or another audit body The cloud service provider can contract the certification body that issued the previous certificate or another certification body. If the application is submitted in good time, the certification body can issue the new certificate for the date immediately following the date of expiry of the previous certificate.

§ 5.4 Monitoring

(1) For the duration of the certificate's validity, the cloud service must be monitored in the form of an annual interim audit as defined in Section 3.6.

(2) The certification body shall remind the cloud service provider and the audit body in good time of the impending interim auditt and shall indicate the consequences of failure to perform the interim audit (Section 5.6). If the interim audit is not performed within the time frame defined in Section 3.6 (3), the certification body shall take measures as set out under Section 5.6 (3 - 7).
(3) The certification body shall assess the interim audit report. Section 4.3 shall apply accordingly.
(4) On the basis of the auditor's interim audit report, the certifier's assessment and, where necessary, other findings, the certification body shall decide without undue delay on whether to maintain, restrict, suspend or withdraw the certificate. Section 4.6 (6) shall apply accordingly.

§ 5.5 Certification mark

(1) The issuing of the certificate entitles the cloud service provider to display the certification mark according to Annex 2) for the certified cloud service in accordance with the certification mark conditions of the certification mark owner.
(2) The certification mark may only be displayed while the certificate is valid.
(3) The certification mark only contains the following information:
    a) The graphic certification mark;
    b) The certificate number;
    c) The period of validity;
    d) The wording TCDP with protection class [I, II, III];
    e) Information on the recoverability level [C, B, A].
(4) The certification body shall issue the certification mark and make it available to the cloud service provider graphically in electronic format.

§ 5.6 Restriction, suspension or withdrawal of the certificate

(1) The cloud service provider can apply for the restriction, suspension or withdrawal of the certificate at all times. This application must be issued unless there are serious reasons for not doing so.
(2) The cloud service provider is obligated to notify the certification body without undue delay and in detail if the cloud service provider discovers that the conditions for the issuing of the certificate were not, or are no longer, satisfied.
(3) If, on the basis of information provided by the cloud service provider, the audit body or a third party, or due to other circumstances, the certification body has reason to suspect that the conditions for the issuing of the certificate were not, or are no longer, satisfied, the certification body shall take the necessary action without undue delay to determine whether the conditions were/are satisfied. In particular, the certification body can declare that an interim audit is necessary to maintain the certificate.
(4) If the certification body declares the need for an interim audit, it shall set the cloud service provider a reasonable deadline by which the interim audit must be performed. The certification body must give the cloud service provider a detailed description of

the aspects casting doubt on compliance with the certification prerequisites. The deadline can be extended at the request of the cloud service provider.

(5) The certification body can suspend the certificate for the duration of the determination process. If the certificate is suspended, the certification mark may not be displayed. The cloud service provider must notify its cloud service users of the suspension.

(6) Based on its findings, and, if applicable, on the basis of the interim audit report, the certification body shall take the actions necessary for TCDP compliance. It can restrict, suspend or withdraw the certificate. The certification body shall give the cloud provider the opportunity to comment before it makes its decision. Change certification can be performed at the request of the cloud service provider.

(7) The certificate must be withdrawn if:

a) The certification body discovers that the preconditions for the issuing of the certificate were not met or are no longer met;

b) If an interim audit was not performed at all or not within the timeframe specified under (4);

c) If the TCDP owner discovers that the TCDP does not meet, or no longer meets, the legal requirements of the Federal Data Protection Act or alternative legal regulations replacing these legal requirements. This does not apply if the cloud service provider applies for change certification immediately after a new version of the TCDP and this is implemented without undue delay.

(8) The withdrawal or restriction of the certificate shall take effect three weeks after notification of the decision to withdraw or restrict the certificate. Suspension shall take effect immediately. Section 4.8 shall apply accordingly.

§ 5.7 Cloud service modification

(1) If the cloud service provider or the provider of a component modifies or intends to modify the cloud service or the component thereof and said modification can result in the need to withdraw or restrict the certificate, the cloud service provider shall be obliged to notify the certification body without undue delay of the intended or already implemented change to the cloud service.

(2) If, on the basis of information supplied by the cloud service provider, audit body or a third party, or due to other circumstances, the certification body learns of a change to a certified cloud service which can result in a different assessment of the cloud service as regards the certification issued, the certification body shall take the necessary action without undue delay to determine whether the modified cloud service also satisfies the certification prerequisites. Section 5.6 shall apply accordingly.

Chapter 6: Final provisions

Section 6.1 Continued validity of certificates according to a GDPR standard

(1) The parties involved in the pilot project hope and expect that, on completion of the pilot project, a data protection standard for cloud services on the basis of the General Data Protection Regulation (GDPR) will be developed based on the TCDP model. The aim should be to receive approval by the European Data Protection Board as referred to in Article 42 of the GDPR.

(2) It is the wish of the parties involved in the project that the standard mentioned in (1) will permit a transition of TCDP certificates on the basis of change or transitional certification. The aim is that TCDP certificates can be replaced as seamlessly as possible by certification according to the new standard on the basis of the GDPR when the GDPR applies on 25 May 2018.

(3) The certificate shall lapse with the entry into force of the GDPR on 25 May 2018 unless, by this time, (i) transitional certification has taken place to transition the certificate to a standard that implements the GDPR and corresponds to the TCDP (ii) such a certification procedure is initiated through the conclusion of a corresponding audit agreement or (iii) the European Commission or the European Data Protection Board has established another transitional arrangement and the conditions of said arrangement are satisfied for the continued validity of the certificate.

§ 6.2 Amendments

Amendments to these Rules of Procedure shall be made by the TCDP owner or administrator.