Trusted Cloud

**Trusted Cloud Competence Centre** **13 April 2015**

# Trusted Cloud Data Protection Profile for Cloud Services (TCDP) — Version 0.9

Trusted Cloud

## Contents

Trusted Cloud

# I. Scope and objectives of TCDP

The Trusted Cloud Data Protection Profile (TCDP) is a test standard for the data protection certification of cloud computing services.

## 1. Addressees and function of TCDP

With data protection certificates, IT service providers can prove that their services conform with legal data protection requirements and IT service users can place their trust in the data protection conformity of certified services. Data protection certification to TCDP applies for the collection, processing or use of personally identifiable data under contract (contracted data processing). Under Section 11 of the Federal Data Protection Act (BDSG), the service user as client must be convinced of the processor's adherence to legal requirements. With a certificate confirming that the respective IT service meets these legal requirements, it is far easier for the IT service provider to gain the confidence of the client. Data protection certification is particularly important for the use of cloud services often rendered as standardised services to many users, because it is an efficient way of meeting the legal obligation for compliance assessment.

TCDP sets out the legal data protection requirements for the processor (cloud service provider). It is not concerned with the legal data protection requirements for the client (cloud service user). These key points of data protection certification, also known as compliance certification to distinguish it from other forms of certification, should be regulated under law.

## 2. TCDP and legal regulation of data protection certification

TCDP is a measure to achieve the goal of legally regulated data protection certification. It is based on the Strategy for the Data Protection Certification of Cloud Services drawn up by the working party, Legal Framework for Cloud Computing[i] in the course of action research for the Trusted Cloud Technology Programme.[ii] The pilot project, Data Protection Certification, has enlarged the foundation for legal data protection certifications. As set out in the paper, Modular Certification of Cloud Services, TCDP is designed for modular certification[iii] and certification according to the principles described in the paper, Basic Principles of a Certification Procedure for Cloud Services[iv] drafted by the pilot project, Data Protection Certification for Cloud Services.

TCDP implements the legal requirements of BDSG for contracted data processing and translates them into verifiable standards. It is premised on ISO/IEC Standard 27018, which enlarges the scope of the internationally approved ISO/IEC Standards 27001[vi] and 27002[vii] to include requirements for cloud computing services and in particular for specific data protection.

TCDP makes reference to the ISO/IEC 27018 and ISO/IEC 27002 Standards, where these are suitable for operationalising the legal requirements of BDSG. Where necessary, it modifies and supplements the ISO standards to meet BDSG provisions. The yardstick and guiding principle of TCDP are therefore the legal requirements of BDSG for contracted data processing.

Trusted Cloud

## 3. Inception and application of TCDP

TCDP was developed in the pilot project, Data Protection Certification for Cloud Services, conducted by the Trusted Cloud Competence Centre on behalf of the Federal Ministry of Economic Affairs and Energy. It is currently available as a beta version and is cited as TCDP - v.0.9. On behalf of the Federal Ministry for Economic Affairs and Energy beginning in the summer of 2015, it will be tested and upgraded in pilot certifications by a project for the practical application of data protection certification. TCDP should be available as a final version in the first half of 2016.

TCDP is a test standard available for general use. It provides a specific basis for issuing certificates. TCDP is premised here on certification to the principles set out in the paper, Basic Principles of a Certification Procedure for Cloud Services. As a general requirement, TCDP must be applied in full without any alterations. The publisher reserves the right to administer and upgrade TCDP.

TCDP was developed as part of the Trusted Cloud Technology Programme and focuses on data protection certification for cloud services. As they translate the relevant general legal requirements, the standards can, however, be applied for all kinds of contracted data processing.

TCDP is an essential measure for achieving the goal of European data protection certification under law. By providing basic design elements, it aims at promoting the development of European data protection certification. TCDP, which currently implements the Federal Data Protection Act, can be revised in line with the European General Data Protection Regulation when it is adopted.

Trusted Cloud

## II. Structure and use of TCDP

### 1. Text categories of TCDP

Similar to ISO/IEC 27018 and other standards, TCDP distinguishes between 'requirements' and 'implementation recommendations' and also contains 'statements'.

Requirements denote normative criteria that must be met to obtain a certificate based on TCDP. They are therefore test yardsticks. Wherever TCDP requirements designate controls from ISO/IEC 27018 or ISO/IEC 27002 as 'normative', these controls then become TCDP requirements and must consequently be met. Where an ISO/IEC control is not worded in obligatory terms ('should'), this is to be understood initially also under TCDP as an optional requirement.

Since BDSG makes mandatory requirements throughout, TCDP standards are also regularly worded as such. As, however, ISO/IEC 27018 and ISO/IEC 27002 largely define optional requirements (controls - 'should'), TCDP references to ISO/IEC controls must be translated into mandatory requirements. TCDP therefore adopts two different approaches. In part, TCDP standards make reference to ISO/IEC controls and make plain that as mandatory requirements these are to be construed as normative, that is, with the wording 'shall' not 'should'. In part also, TCDP employs its own wording for the respective requirement and refers in square brackets to the substantive equivalent of ISO/IEC controls. In some cases, it is questionable whether BDSG requirements tally with the ISO/IEC control or this is not apparent from the wording. By employing its own wording for the requirement and referring to ISO/IEC controls as a bracket addition, TCDP makes plain that in the case of possible deviations, the requirement in pursuance of BDSG is normative.

Implementation recommendations are supposed to provide pointers and assistance for understanding and implementing requirements, but do not in themselves constitute a 'normative' requirement.

Implementation recommendations on individual TCDP standards are generally aligned with the protection categories as defined in the related TCDP concept.[viii] Where no specific security category is cited in a TCDP standard, this means that implementation recommendations apply for all security categories alike. Where implementation recommendations distinguish among security categories, they subsume the subordinate one(s), where these do not contradict each other.

Where expedient, implementation recommendations include those of the ISO standards by reference. The same applies accordingly for requirements.

Trusted Cloud

To limit the amount of text, the implementation recommendations are in part tabulated and summarised in key points, particularly the extensive recommendations on technical and organisational measures in the third section (TCDP No. 21 ff). The tabulation also includes the implementation recommendations of the ISO standards, each indicated in bold type.

The 'statements' are intended for easier understanding of the requirements and their derivation from the act.

## 2. Application and citation format of ISO Standard

As TCDP refers to ISO/IEC 27018 and ISO/IEC 27002, its application calls for familiarity with these standards. A prior certification to ISO/IEC 27001 is not a prerequisite for TCDP. Because TCDP makes use of the taxonomy and terminology of the ISO/IEC 27002 family, a TCDP certification is much easier when this kind of certification has already been issued.

The ISO/IEC standards are cited in their current edition (ISO/IEC 27018: 2014; ISO/IEC 27002: 2013) as appended in the references. For easier reading, TCDP cites the standards in the text as ISO/IEC 27018 or ISO/IEC 27002 for short.

ISO/IEC 27018 proceeds from ISO/IEC 27001 and ISO/IEC 27002 and often makes reference to ISO/IEC 27002 controls. As far as possible in these cases,[1] TCDP refers both to the referring ISO/IEC 27018 control and the normative ISO/IEC 27002 control.

[1] In some cases, owing to their different taxonomies the ISO/IEC 27018 reference to ISO/IEC 27002 is less precise than in TCDP. In this case, TCDP does not cite the reference in ISO/IEC 27018. For example, TCDP No. 23 (Data transport) makes reference to ISO/IEC 27002 No. 8.2. The reference by ISO/IEC 27018 No. 8 to ISO/IEC 27002 No. 8 is far more detailed and is therefore not separately cited in TCDP No. 23.

## III. Table of standards

| BDSG standard | Contents of standard | Brief description | TCDP number |
|---|---|---|---|
| **Section 11** | **Requirements for contract** | **Compliance with legal requirements for contract** | 1 |
| Section 11(2) 2nd sentence | Service delivery under contract | Service delivery only under data processing contract | 1.1 |
| Section 11(2) 2nd sentence | Form of contract | Contract to be concluded in writing | 1.2 |
| Section 11(2) 2nd sentence No. 1 | Contract subject and term | Contract subject and term to be specified | 1.3 |
| Section 11(2) 2nd sentence No. 2 | Scope/type/purpose/stakeholders | Scope/type/purpose of collection, processing, use and stakeholders to be specified | 1.4 |
| Section 11(2) 2nd sentence No. 3 | Technical and organisational measures | Measures to be taken under Section 9 of BDSG to be specified | 1.5 |
| Section 11(2) 2nd sentence No. 4 | Correction/deletion/blockage | Provisions on correction, deletion and blockage of data on client instruction to be specified | 1.6 |
| Section 11(2) 2nd sentence No. 5 | Obligations of processor | Obligations of processor to be specified, particularly controls | 1.7 |
| Section 11(2) 2nd sentence No. 6 | Subcontractors | Permission for processor to engage subcontractors to be specified | 1.8 |
| Section 11(2) 2nd sentence No. 7 | Client rights and processor obligations | Client control rights and processor obligations to tolerate and cooperate to be specified | 1.9 |
| Section 11(2) 2nd sentence No. 8 | Notification of breaches | Notification of which breaches of provisions or contractual specifications to be specified | 1.10 |
| Section 11(2) 2nd sentence No. 9 | Client authority to issue instructions | Client authority to issue instructions to processor to be specified | 1.11 |

| | | | |
|---|---|---|---|
| Section 11(2) 2nd sentence No. 10 | Obligations to return | Return of data carriers and deletion of data by processor to be specified | 1.12 |
| **Sections 11, 5** | **Relationship between cloud service provider and user** | **Organisational measures to be taken by processor for service delivery in keeping with data protection requirements** | |
| Section 11(3) 1st sentence | Obligation to act on instructions | No collection/processing/use of data other than as instructed by client | 2 |
| Section 11(3) 2nd sentence | Obligation to report | Contractor obligation to report if client instruction contravenes BDSG or other data protection provisions | 3 |
| Section 11(2) 2nd sentence No. 6 | Subcontractors (right to issue subcontracts) | Contractor must provide evidence of the proper engagement of subcontractors | 4 |
| Section 11(4) | In-company data protection officer and legal requirements | Contractor obligations under Sections 5, 9, 43(1) Nos. 2, 10 and 11, (2) Nos. 1 to 3 und (3) and Sections 44, Section 4f, 4g and 38 | 5 |
| Section 11(2) 2nd sentence No. 4 | Correction/blockage and deletion of data | Provisions to be made to facilitate the correction, blockage and deletion of data | 6 |
| Section 11(2) 2nd sentence No. 8 | Obligation to report | Breaches of legal or contractual provisions must be reported | 7 |
| Section 11(2) 2nd sentence | Client control rights/Contractor obligations to tolerate and cooperate | Contractor must maintain procedures for client audit | 8 |
| Section 11(2) 2nd sentence No. 10 | Obligations to return | Contractor must provide evidence of return procedures | 9 |
| Section 5 | Data confidentiality | Contractor must oblige personnel to observe data confidentiality | 10 |
| **Section 9 in conjunction with Annex** | **Technical-organisational security of cloud service** | **Assurance of data processing security** | |
| 2nd sentence No. 1 of Annex to Section 9 | Entry control | Refusal of entry for unauthorised persons to data processing installations | 21 |
| 2nd sentence No. 2 of Annex to Section 9 | Equipment access control | Prevention of access for unauthorised persons to data processing systems | 22 |

Trusted Cloud

| | | | |
|---|---|---|---|
| 2nd sentence No. 3 of Annex to Section 9 | Data access control | Assurance that authorised persons only have access to their own data segment | 22 |
| 2nd sentence No. 4 of Annex to Section 9 | Transfer control | Protection of data during transport, storage and transmission from access by unauthorised persons | 23 |
| 2nd sentence No. 5 of Annex to Section 9 | Input control | Assurance that users who input, alter or remove personally identifiable data can be subsequently traced | 24 |
| 2nd sentence No. 6 of Annex to Section 9 | Job control | Assurance that personally identifiable data may only be processed as instructed by client instructions/directions/orders/dir | 25 |
| 2nd sentence No. 7 of Annex to Section 9 | Availability control | Assurance that personally identifiable data are not destroyed or lost by accident | 26 |
| 2nd sentence No. 8 of Annex to Section 9 | Separate processing | Assurance that collected data can be processed separately in keeping with the respective purpose | 27 |
| Section 9 | Cryptography | Requirements for the application of cryptographic methods | 28 |

Trusted Cloud

# IV. Requirements and implementation recommendations

## 1. Contractual arrangements for contracted data processing

### TCDP No. 1 - Contractual basis

The cloud service provider must take measures to ensure that it renders its service to the cloud service user under a contract that meets the legal requirements of BDSG for contracted data processing. The following requirements are designed to assure this.

Numbers 1.3 to 1.12 of TCDP can be met by the cloud service provider offering a contract that meets the cited requirements. Specimen contracts can be helpful when preparing this kind of contract.

### TCDP No. 1.1 - Service delivery under contract

*Requirement*

By making appropriate organisational preparations, the cloud service provider shall ensure that the cloud service is not performed until a contract has been concluded with the cloud service user that meets the requirements of TCDP No. 1.

### TCDP No. 1.2 - Form of contract

*Requirement*

The cloud service provider shall offer to conclude a written contract for contracted data processing.

*Implementation recommendation*

Evidence of the willingness to conclude a written contract can, for example, be provided by a draft contract (pro forma contract) and a procedure for concluding the contract in writing.

### TCDP No. 1.3 - Subject and term of contract

*Requirement*

The subject and term of the contract shall be stipulated in the cloud contract.

*Implementation recommendation*

The contract should either specify a definite period of time or make clear that it is to be concluded for an unlimited term. Contracts entered into for an unlimited term should include provisions on cancellation, particularly period of notice.

The cloud service provider can ensure this by providing for a draft contract (pro forma contract) containing this information and adopting a procedure for concluding the contract with this information included.

## TCDP No. 1.4 - Type and purpose of data processing

*Requirement*

The scope, type and purpose of the envisaged collection, processing or use of data, the type of data and the stakeholders shall be stipulated in the cloud contract.

*Implementation recommendation*

These individual details need not cater for each specific individual case, but they should be precise enough to ensure the transparency of specific permissible data use as part of contracted data processing.

Depending on the type of cloud service, specifications can be made in different ways. Particularly in the case of the standard services under Software as a service (SaaS), where the type and purpose of data are already apparent from the purpose of the programme, reference to the programme description in the documentation can already suffice as specification. With more complex or less specified services (e.g. Platform as service - PaaS), regular conferral with the cloud service user is necessary. This can, for example, be organised by means of an electronic form, where the cloud service user enters the requisite information.

## TCDP No. 1.5 - Technical and organisational measures

*Requirement*

1. Technical and organisational measures to be taken under TCDP Nos. 21 - 28 shall be stipulated in the cloud contract.
2. The cloud service provider shall make a statement on the protection category to be guaranteed by it.

*Implementation recommendation*

This can be specified in an annex appended to the contract. Information on the implementation of TCDP Nos. 21 - 28 (Section 9 of BDSG and Annex) can pertain to security objectives, while the specific measures for objective achievement can be left to the cloud service provider. This should be specified in the form of an information security concept appended to the contract as annex.

It is important for the cloud service user to know to which protection requirement category the cloud service belongs as provided for in the Trusted Cloud protection category concept. It is therefore advisable to explicitly include in the cloud contract the guarantee of a certain information security category in keeping with the Trusted Cloud concept for information security categories.

## TCDP No. 1.6 - Correction, deletion and blockage of data

*Requirement*

The procedures for the correction, deletion and blockage of data (TCDP No. 6) shall be stipulated in the cloud contract.

*Implementation recommendation*

It is advisable to specify deletion periods and methods.

## TCDP No. 1.7 - Obligations of cloud service provider

*Requirement*

The cloud contract shall specify the legal data protection standards applicable to the cloud service provider under Section 11(4) of BDSG.

*Statement*

Section 11(2) 2nd sentence No. 5 of BDSG requires that the cloud contract must clearly specify which of the legal requirements cited therein apply to the cloud service provider as processor.

*Implementation recommendation*

It is sufficient for the cloud contract to specify the legal provisions applicable to the cloud service provider. It is expedient and customary not to just cite these with reference to section and paragraph, but also to describe the contents or quote the wording.

Trusted Cloud

## TCDP No. 1.8 - Subcontractors

*Requirement*

1. The cloud contract shall specify any possible authorisation to issue subcontracts.
2. When subcontracting, the cloud service provider shall give an undertaking to the cloud service user to comply with the requirements under TCDP No. 4.

*Statement*

Subcontractors may only be engaged with the consent of the cloud service user, need not, however, be explicitly named in the contract.

## TCDP No. 1.9 - Control rights of cloud service user

*Requirement*

The control rights of the cloud service user (TCDP No. 8) and the corresponding obligations of the cloud service provider to tolerate and cooperate shall be stipulated in the cloud contract.

## TCDP No. 1.10 – Reporting breaches

*Requirement*

The cloud contract shall specify which breaches by the cloud service provider or its personnel (cf. TCDP No. 7) of provisions on the protection of personally identifiable data or contractual provisions must be reported.

*Implementation recommendation*

As a minimum requirement, the cloud contract must contain the obligation to give notification of data protection breaches without delay. It is also advisable to specify in the contract the mode and communication channel for notification.

## TCDP No. 1.11 – Cloud service user authority to issue instructions

*Requirement*

The cloud contract shall stipulate the scope of authority available to the cloud service user to issue instructions to the cloud service provider.

*Implementation recommendation*

The cloud service user must be granted the prerogative to issue individual instructions. It is advisable to make provision in the contract for the individual instruction to be issued in

writing and confirmed by the cloud service provider. The contract should precisely identify which persons are authorised to issue individual instructions. These can be mentioned by name in the cloud contract.

## TCDP No. 1.12 - Return and deletion of data

*Requirement*

The cloud contract shall specify the obligations of the cloud service provider to return and delete data (TCDP No. 9).

*Implementation recommendation*

At the least, the cloud contract should specify the obligations cited in TCDP No. 9. It is advisable to frame detailed provisions. This can also be done by making reference to the relevant principles of the cloud service provider.

## 2. Relationship between cloud service provider and user

### TCDP No. 2 - Cloud service provider obligation to follow instructions

*Requirement*

By taking suitable measures, the cloud service provider shall ensure in the performance of the service that he is obliged to only collect, process and use the data as instructed by the cloud service user.

*Statement*

The obligation of the cloud service provider to act on instructions is regulated at three points in the Federal Data Protection Act (Section 11(2) 2nd sentence No. 9, (3) first sentence, Annex to Section 9 No. 4 of BDSG). TCDP consequently also clarifies the obligation to follow instructions at three points: TCDP No. 2 makes plain that the cloud service provider must undertake to follow instructions, TCDP No. 1.11 designates this as a necessary component of the cloud contract and TCDP No. 25 obliges the cloud service provider to take technical and organisational measures to ensure that instructions are followed.

*Implementation recommendation*

By means of an organisational procedure, the cloud service provider should ensure in the contract that he enters into an obligation to the cloud service user to conduct the contracted data processing solely in the performance of instructions from the cloud service user. This can be arranged with the help of a pro forma contract (cf. TCDP No. 1.11). The cloud service provider should also have an organisational measure in place to make sure that no cloud service is carried out before this binding commitment has been made.

Instructions comprise the specification of the data processing by the cloud service provider. This can be done by reaching an agreement on the functionalities of the cloud service, which can be made in the cloud contract, for example, by reference to the documentation of functionalities (cf. TCDP No. 1.11).

In addition, the cloud service user must be accorded the right to issue individual instructions (cf. TCDP No. 1.11).

### TCDP No. 3 - Obligation to raise an objection

*Requirement*

By taking appropriate measures, the cloud service provider shall ensure that he notify the cloud service user without delay if he is of the view that an instruction by the cloud service

Trusted Cloud

user breaches legal data protection provisions and await his decision before carrying out the instruction.

*Statement*

Under the principles of outsourced data processing, the responsibility for data protection conformity in processing lies with the cloud service user, which is consequently also authorised to issue instructions to the cloud service provider. Nevertheless, the cloud service provider may not indiscriminately execute an instruction whose lawfulness he has reason to doubt. Rather, Section 11(3) 2nd sentence of BDSG obliges him to lodge an objection in such cases. He must warn the cloud service user, if he has misgivings as to the legality of an instruction under current data protection law and await the decision of the cloud service user.

*Implementation recommendation*

The cloud service provider can arrange for and document a procedure where personnel of the cloud service provider check instructions for data processing that diverge from the customary or expected processing in the respective service or give cause for misgivings in another respect and in the case of persistent doubts can submit this assessment for decision by the cloud service user prior to execution. It is advisable to arrange for the cloud service user to take an explicit decision in writing. This may need to be regulated in the cloud contract.

## TCDP No. 4 - Subcontractors

*Statement*

Cloud service providers regularly perform cloud services by engaging subcontractors that are integrated in this capacity in outsourced data processing. As subcontractors in turn often resort to other subcontractors, this frequently results in multilevel subcontracting relationships.

It is generally permissible to engage subcontractors and sub-subcontractors. As processor, however, the cloud service provider must ensure that the requirements for outsourced data processing are adhered to by all subcontractors at all levels.

## TCDP No. 4.1 - Basis for engaging subcontractors

*Requirement*

1. The cloud service provider shall ensure that a cloud service involving subcontractors is only performed for a cloud service user, if and insofar the latter has given its consent for this.

*Implementation recommendation*


If it engages subcontractors, the cloud service provider can meet these requirements by arranging for a procedure where the service is not performed for the cloud service user until its consent has been verified, usually by concluding the cloud computing contract with the inclusion of a relevant provision (cf. TCDP No. 1.8).

## TCDP No. 4.2 - Information of cloud service user

*Requirement*

1. The cloud service provider shall inform the cloud service user of the identity of all subcontractors it engages (including the official business address).
2. The cloud service provider shall inform the cloud service user of the identity of all sub-subcontractors (including official business address) engaged by subcontractors it has commissioned. This shall apply for all levels of sub-subcontracting.
3. The cloud service provider shall inform the cloud service user of all changes in the identity of subcontractors or sub-subcontractors, especially new additional subcontractors or sub-subcontractors.

*Implementation recommendation*

The information can be provided by electronic means, such as a link to a (secure) segment of the website containing this information. Information about changes can be communicated by electronic means, by email, for example, or in another way.

## TCDP No. 4.3 - Contractual arrangements for sub-contracting

*Requirement*

1. The cloud service provider shall ensure that its subcontractors do not perform their services without an effective contract for subcontracted data processing.
2. The cloud service provider shall oblige its subcontractors to ensure that their sub-subcontractors are not engaged without an effective subcontracted data processing contract and oblige their sub-subcontractors to do the same.

*Implementation recommendation*

The cloud service provider can meet the requirement in paragraph 1 by arranging for a procedure where the subcontractor is not engaged in the service until the subcontracted data processing contract between the cloud service provider and the subcontractor has been verified.

The requirement in the second paragraph can be met, for example, by including this obligation in the subcontracted data processing contract.

Trusted Cloud

## TCDP No. 4.4 - Selection and supervision of subcontractors

*Requirement*

1. The cloud service provider shall ensure that it only engages subcontractors that can provide an assurance of compliance with legal data protection requirements for the service to be rendered by them.
2. The cloud service provider shall satisfy himself that its subcontractors meet the legal data protection requirements for the service to be rendered by them.

*Implementation recommendation*

The requirements in paragraph 1 and 2 can also be met if the cloud service provider is satisfied that the subcontractor (still) meets the requirements by examining a (valid) certificate.

## TCDP No. 4.5 – Instructions by the cloud service user

*Requirement*

1. The cloud service provider shall ensure that the instructions of the cloud service user are conveyed to the subcontractors.
2. The cloud service provider shall oblige its subcontractors to assure adherence to the instructions from the cloud service user and oblige their sub-subcontractors to do the same.
3. The cloud service provider shall verify that subcontractors and their sub-subcontractors comply with the instructions of the cloud service user.

*Statement*

If the instructions of the cloud service user are forwarded along the chain of (subcontracting) processors, the cloud service provider bears overall organisational responsibility for compliance with the instructions of the cloud service user.

*Implementation recommendation*

The cloud service provider can meet the requirement in paragraph 1 by establishing a procedure where the instructions of the cloud service user must be forwarded to the subcontractors, technically, for example, through automatic transfer, or by means of an organisational procedure where instructions are processed manually.

The requirement in paragraph 2 can, for example, be met by including this obligation in the subcontracted data processing contract. The cloud service provider can, for example, meet the requirement in paragraph 3 by satisfying itself with suitable measures (perusal of certificates or its own appraisals) that instructions are forwarded and carried out.

Trusted Cloud

## TCDP No. 5 - In-company data protection officer and legal requirements

*Requirement*

By taking suitable measures, the cloud service provider shall make provision for guaranteeing compliance with the legal data protection requirements under Sections 4f and 4g and/or Section 18 of BDSG and/or federal state data protection acts.

*Statement*

Section 11(4) of BDSG imposes certain legal requirements on cloud service providers as processors. Sections 9 and 11 of BDSG cited therein are implemented by the other requirements of TCDP; as elements of an administrative infringement and/or a criminal offence, Section 43 and 44 of BDSG are not relevant for certification, nor are Section 38 of BDSG (Supervisory authority) and/or Sections 24-26 of BDSG (Federal Commissioner for Data Protection and Freedom of Information) and/or the relevant provisions of the federal state data protection acts. The provisions on the data protection officer (Sections 4f and 4g of BDSG) and/or compliance (Section 18 of BDSG and/or federal state data protection acts) are implemented in TCDP No. 5 and the provisions on data confidentiality (Section 5 of BDSG) in TCDP No. 10.

If the cloud service provider is obliged to appoint a data protection officer, it must meet the requirements for an effective appointment by ensuring that he is independent, reliable and can draw on the requisite expertise. To do this, the cloud service provider must conduct a prior appraisal of the suitability of the prospective data protection officer to confirm that he satisfies the requirements for reliability (especially with regard to possible conflicts of interest) and he possesses the requisite expertise to meet the specific needs of the appointing cloud service provider. The prospective data protection officer must also collaborate in this procedure (own assessment of requirements, information on professional qualifications, conflicts of interest, etc.).

*Implementation recommendation*

For the purpose of establishing a data protection organisation, by taking organisational measures the cloud service provider must ensure that the data protection officer can perform his tasks independently and in keeping with legal provisions.

| Security category | Implementation recommendations |
|---|---|
| I, II, III | – Documentation of systems, procedures and processes applied for the respective cloud service (software, hardware, organisational units involved, roles and service providers)<br>– Exact description of all technical and organisational measures taken (e.g. in a data protection concept)<br>– Effective appointment of a data protection officer (DPO):<br>o Documentation of the aptitude test by the DPO and cloud service provider, especially his expertise and reliability for the type and scope of data processing and possible conflicts of interest<br>o Written certificate of appointment signed by both parties<br>o Evidence of the requisite independence of the DPO. Where an external DPO is appointed, evidence of independence from his employer may be required.<br>o Evidence that the DPO has the requisite resources at his disposal to perform his task and is not subject to conflicts of interest, in the case of an external DPO disclosure of the supervised responsible units and the related necessary time input<br>o Direct organisational subordination of the data protection officer to the head of the cloud service provider<br>– Suitable integration of the DPO and the IT/information security officer in the organisation of the cloud service provider<br>– Adequate time schedule for the DPO to cope with the protection needs and number of clients (possible support from data protection coordinators)<br>– Annual planning and allocation of budgets for DPO activities (e.g. to draw on external expertise, further training).<br>– Regular, e.g. quarterly, internal audits and reporting by DPO |

## TCDP No. 6 - Correction, deletion and blockage of data

*Requirement*

By taking suitable measures, the cloud service provider shall ensure that the cloud service user can carry out the correction, blockage and deletion of personally identifiable data itself or have this carried out by the cloud service provider [ISO/IEC 27018 No. A.1.1.].

*Statement*

Pursuant to Section 11(2), 2nd sentence, No. 4 of BDSG, the client must be given the possibility to correct, delete or block personally identifiable data or in any case arrange for these measures, so that it can meet its obligations arising from Section 35 of BDSG. In

substance, this requirement is actually entailed in ISO/IEC 27018 No. A.1.1., even though blockage is not explicitly mentioned, for example.

*Implementation recommendation*

The cloud service provider should arrange for and document a procedure to regulate the correction, deletion and blockage of data and support for the client with information exchange. The cloud service provider can meet this requirement, for example, by providing the cloud service user with the relevant data for information exchange on request and enabling it to correct, delete and block data in self-service.

## TCDP No. 7 – Obligation to report data protection breaches

*Requirement*

By taking suitable measures, the cloud service provider shall ensure that the cloud service user is notified without delay of breaches of legal or contractual data protection requirements where an unlawful transfer, disclosure or alteration of personally identifiable data cannot be ruled out.

*Statement*

TCDP No. 7 is largely equivalent in substance to ISO/IEC 27018 No. A.9.1., but in pursuance of the legal provisions expands on this by requiring that breaches must be reported even if an unlawful transfer, disclosure or alteration of personally identifiable data has not been ascertained but at the same time cannot be ruled out.

*Implementation recommendation*

| Security category | Implementation recommendations |
|---|---|
| I | – **ISO/IEC 27018 No. A.9.1**<br>– Specification of responsibilities and competencies for verifying the obligation to report<br>– Contact point within adequate reach<br>– Description and implementation of the procedure for reporting events and notifying the client of breaches in data protection and security<br>– Documentation of reported breaches and notifications made to the client |
| II, III | – Description and implementation of the procedure for notifying the client of data protection events to meet the obligation under Section 42a of BDSG. |

Trusted Cloud

## TCDP No. 8 - Support for controls by cloud service user

*Requirement*

By taking suitable measures, the cloud service provider shall ensure that the cloud service user can satisfy himself of compliance with the technical and the organisational requirements under Section 9 of BDSG and can perform the control rights stipulated in the cloud contract (cf. TCDP No. 1.9).

*Statement*

Under Section 11 of BDSG, the cloud service user is legally bound to satisfy itself of compliance with the technical and organisational requirements by the cloud service provider. This requirement can be generally met through examination of the certification, but it is assumed that the cloud service user must be accorded the right of verification regardless of this.

*Implementation recommendation*

The cloud service provider can provide for and document a procedure where requests by the cloud service user are dealt with and the requisite collaboration of the cloud service provider is assured. Provision should be made here to make information on the technical and organisational measures available to the cloud service user, reply to questions and enable on-site inspection.

## TCDP No. 9 - Return and deletion of data

*Requirement*

By taking suitable measures, the cloud service provider shall ensure that the data carriers supplied are returned and data stored by it are deleted after completion of the contract on the instruction of the cloud service user [ISO/IEC 27018 No. A.9.3].

*Implementation recommendation*

The cloud service provider can arrange for and document a procedure to regulate the return of the data carriers on completion of the contract. The cloud service provider can also meet the requirement by enabling the cloud service user to delete the data in self-service.

## TCDP No. 10 - Data confidentiality

*Requirement*

The controls of ISO/IEC 27018, Nos. A.10.1. and 7.2.2 and ISO/IEC 27002, Nos. 7.2.1 and 7.2.2 shall be normative as obligatory requirements.

*Implementation recommendation*

| **Security category** | **Implementation recommendations** |
|---|---|
| I, II, III | - **ISO/IEC 27018 No. A.10.1**<br>- **ISO/IEC 27002 No. 7.1.2**<br>- **ISO/IEC 27002 No. 7.2.2**<br><br>**Notes**<br>The obligation to data confidentiality need not necessarily make up a formal constituent of or be appended to the contract of employment. The instruction and undertaking are not prerequisite to entering into an employment relationship and need not be made until commencement of data-processing activity. |

## 3. Technical and organisational measures

### TCDP No. 21 - Secure area and entry control

*Requirement*

The controls of ISO/IEC 27018 No. 11.1 and ISO/IEC 27002 No. 11.1 shall be normative as obligatory requirements.

*Implementation recommendation*

| Security category | Implementation recommendations |
|---|---|
| I | - **ISO/IEC 27002 No. 11.1.1 a)**<br>- **ISO/IEC 27002 No. 11.1.1 b)**<br>- **ISO/IEC 27002 No. 11.1.1 c)** |
| II | - **ISO/IEC 27002 No. 11.1.1 d)**<br>- No window in IT and **technical** zone |
| III | - **ISO/IEC 27002 No. 11.1.1 e)**<br>- **ISO/IEC 27002 No. 11.1.1 f)**<br>- **ISO/IEC 27002 No. 11.1.1 g)**<br>- Division of the computer centre into secure zones with separate entry regulations<br>- Secure zones are designed according to the onion-skin model (each secure zone is fully enclosed by the preceding one).<br>- Entry into a secure zone and IT and technical segments of the computer centre is specifically restricted by means of an appropriate entry control system, is managed by an entry control facility and is kept under closed surveillance.<br>- IT and technical segments are secured with a burglary alarm system. In addition, all openings, such as shafts, low access passages or vents into the respective secure zones are secured with a burglary alarm system. IT segments are monitored with appropriate movement detectors.<br>- Entry to all rooms in the computer centre is under video surveillance, secured by entry control facilities and entry is registered.<br>- The perimeters of the computer centre are under full, continuous video surveillance.<br>- The security control centre is permanently (7x24 hours) staffed by dedicated and trained security personnel.<br>- Security personnel conduct and record patrols of the centre at irregular intervals.<br>- Identification and registration of individuals and carried items<br>- Separate securing of hardware (servers, network elements, etc).<br>- There are no windows in the computer centre (one exception being the reception area).<br>- Only registered data processors and carriers may be taken into the computer centre. |

## TCDP No. 22 - Logical access to data processing equipment and access to data

*Statement*

The requirements for entry and access controls cited in the Annex to Section 9 of BDSG, Nos. 2 and 3 can hardly be separated in practice and are also considered together in the ISO standards, for example. TCDP also adopts this approach.

*Requirement*

1. The controls of ISO/IEC 27018, Nos. 9 and 12.4 and ISO/IEC 27002, Nos. 9 12.4 and 13.1.1 shall be normative as obligatory requirements.
2. The requirements in paragraph 1 shall also apply for backup copies.

*Implementation recommendation*

Suitable measures must be selected for implementation and carried out in an appropriate way. Account must be taken of the possibility that certain administrative activities in access management can be assigned to the user when using cloud services (cf. ISO/IEC 27018, No. 9.2).

| **Security category** | **Implementation recommendations** |
|---|---|
| I | - **ISO/IEC 27018 No. 12.4**<br>- **ISO/IEC 27002 No. 9.1.1**<br>- **ISO/IEC 27002 No. 9.1.2**<br>- **ISO/IEC 27002 No. 9.2.1 a-b)**<br>- **ISO/IEC 27002 No. 9.2.2 a)**<br>- **ISO/IEC 27002 No. 9.2.3 a-c)**<br>- **ISO/IEC 27002 No. 9.2.4 a-b)**<br>- **ISO/IEC 27002 No. 9.2.5**<br>- **ISO/IEC 27002 No. 9.3.1**<br>- **ISO/IEC 27002 No. 9.4.1**<br>- **ISO/IEC 27002 No. 9.4.2 i-l)**<br>- **ISO/IEC 27002 No. 9.4.3**<br>- **ISO/IEC 27002 No. 9.4.4 a-d)**<br>- **ISO/IEC 27002 No. 9.4.5**<br>- **ISO/IEC 27002 No. 12.1.4 a-b)**<br>- Rights and role concept (cf. also ISO/IEC 27002 No. 9.1.1)<br>- Automatic log-off of workplace computer or limited function (operational or time limit)<br>- Narrow restriction of authorised users.<br>- Application of methods for separating data types (e.g. separation of user and operating, personally identifiable data and non-personally identifiable data)<br>- Regular evaluation of protocols |

| | |
|---|---|
| II | - I**SO/IEC 27002 No. 6.1.2**<br>- **ISO/IEC 27002 No. 9.2.1 c), d)**<br>- ISO/IEC 27002 No. 9.2.1 e) with the proviso that users that are registered and de-registered by the administrator of the cloud service user in self-self-service cannot be centrally identifiable.<br>- **ISO/IEC 27002 No. 9.2.1 f-h)**<br>- ISO/IEC 27018 No. 9.2.1 can be addressed, for example, by displaying the last login so that the user can detect whether the registration data have been compromised. An option should also be available for assigning a new user name and password.<br>- **ISO/IEC 27002 No. 9.2.2 b-h)**<br>- **ISO/IEC 27002 No. 9.2.3 e-f)**<br>- **ISO/IEC 27002 No. 9.2.4 c-e)**<br>- **ISO/IEC 27002 No. 9.4.2 a-e)**<br>- **ISO/IEC 27002 No. 9.4.3**<br>- **ISO/IEC 27002 No. 9.4.4 e-i)**<br>- **ISO/IEC 27002 No. 12.1.4 c-g)**<br>- ISO/IEC 27018 No. 12.3 (last paragraph: Policy for erasure of PII contained in the backup)<br>- **ISO/IEC 27018 No. 12.4.2**<br>- **ISO/IEC 27018 No. A.4.1**<br>- **ISO/IEC 27002 No. 13.1.1**<br>- ISO/IEC 27018 No. A.9.3: Data deleted by the cloud service user should be shredded to at least a particle size equivalent to DIN 66399 Level 2.<br>- Implementation of protective measures for metadata (no restriction on protection of content data).<br>- Sanctions on faulty access attempts (time locks, invalid chipcard, etc).<br>- Encryption and digital signatures |

| | |
|---|---|
| III | - **ISO/IEC 27002 No. 9.4.5**<br>- ISO/IEC 27002 No. 9.2.3 d): If an access secret (registration, invitation link, etc) is transferred on an insecure channel, a second factor must be available independent of this channel.<br>- Re ISO/IEC 27002 No 9.2.4: On servers or network elements where unencrypted data of cloud service users are processed, no access privilege may be assigned. On servers or network elements where no or only encrypted data of cloud service users are processed, an access privilege should only be assigned as required, i.e. for a defined and documented maintenance task, for example.<br>- **ISO/IEC 27002 No. 9.4.2 f-h)**<br>- Re ISO/IEC 27002 No. 9.4.4: Technologies should be applied to guarantee that access to servers or network elements with particular privileges, i.e. that enable access to the data of cloud service users, contain state-of-the art mechanisms for the separation of powers that go beyond customary organisational measures.<br>- Re ISO/IEC 27018 No. 12.4.2: In keeping with state-of-the-art technology, these implementation recommendations for organisational measures can also be replaced by the technical measures for log data and/or metadata protection.<br>- ISO/IEC 27002 No. 6.1.2: State-of-the-art technology should enforce separation of duties. In particular: “Care should be taken that no single person can access, modify or use assets without authorisation or detection.”<br>- ISO/IEC 27002 No. 12.3.1 f: The encryption of data in the backup should be organised so that the processor has no access to read keys. Readability of personally identifiable data should only be restorable with keys held by the cloud service user.<br>- ISO/IEC 27018 No. 12.4.2: The measure recommended under this number to regularly delete log information should be carried out automatically in this security category.<br>- ISO/IEC 27018 No. A.5.1: In this security category, data should be able to be processed that are protected against confiscation. As far as possible therefore, the release of personally identifiable data should be prevented by technical measures in keeping with state-of-the-art technology.<br>- ISO/IEC 27018 No. A.9.3: Data deleted by the cloud service user should be shredded to at least a particle size equivalent to DIN 66399 Level 3.<br>- Interception-proof equipment and communication lines<br>- Low-emission monitors<br>- Signature methods to identify a user<br>- Separate securing of hardware (servers, network elements, etc)/Specification of secure areas<br>- Attendance records |

## TCDP No. 23 – Data transfer and storage

*Requirement*

The cloud service provider shall take suitable measures to ensure that personally identifiable data cannot be read, copied, altered or removed without authorisation during their electronic transmission or transportation or storage on a data carrier and the group of envisaged recipients of transmitted personally identifiable data can be traced. Moreover, arrangements must be made for logging transmission operations [ISO/IEC 27018 Nos. 10, A.10.4, 10.5, 10.6, 10.9; ISO/IEC 27002 Nos. 8.3, 10, 12.4.1, 12.4.2, 12.4.3, 13].

*Statement*

In any event, the cited ISO/IEC 27018 and ISO/IEC 27002 Standards essentially meet the substantive legal requirements for (data) transmission control (Section 9 1st sentence of BDSG in conjunction with Annex No. 4). TCDP supplements the ISO standards with measures for the prior delimitation of the group of recipients and logging transmissions to recipients that are not concurrent users of the system, as these measures are not explicitly addressed in the ISO standards.

*Implementation recommendation*

| Security category | Implementation recommendations |
|---|---|
| I | - **ISO/IEC 27018 No. A.10.4**<br>- **ISO/IEC 27018 No. A.10.5**<br>- **ISO/IEC 27018 No. A.10.6**<br>- **ISO/IEC 27018 No. A.10.9**<br>- **ISO/IEC 27002 No. 8.3**<br>- **ISO/IEC 27002 No. 10.1.1**<br>- **ISO/IEC 27002 No. 10.1.2**<br>- **ISO/IEC 27002 No. 12.4.1**<br>- **ISO/IEC 27002 No. 12.4.2**<br>- **ISO/IEC 27002 No. 12.4.3**<br>- **ISO/IEC 27002 No. 13.1.1 a-b)**<br>- **ISO/IEC 27002 No. 13.1.2 a-c)**<br>- **ISO/IEC 27002 No. 13.1.3** |
| II | - ISO/IEC 27002 No. 10.1.2: Keys should be managed so that the cloud service provider and operator have no access to keys that permit of reading personally identifiable data of cloud service users.<br>- **ISO/IEC 27002 No. 13.1.1 c-g)**<br>- ISO/IEC 27002 No. 13.1.3: Separation of networks used for the operation of the operational framework and application software |

| | |
|---|---|
| III | - ISO/IEC 27002 No. 13.2.3: Particular attention should be paid to these implementation recommendations as part of the client service process in the communication of the cloud service provider with cloud service users. |

## TCDP No. 24 - Transparency of data processing

*Requirement*

The controls of ISO/IEC 27018 No. 12.4 and ISO/IEC 27002 No. 12.4. shall be normative as obligatory requirements.

*Statement*

The controls of ISO/IEC 27002 No. 12 to which ISO/IEC 27018 No. 12 refers correspond in substance to the legal requirements for input control (Section 9 1st sentence in conjunction with No. 5 of the Annex to Section 9 1st sentence of BDSG) and operationalise these to an adequate extent. The transparency of all data alterations is of special importance for the cloud service provider. This is why TCDP No. 24 designates the controls of ISO/IEC 27002 as obligatory ('shall').

*Implementation recommendation*

| **Security category** | **Implementation recommendations** |
|---|---|
| I, II, III | - **ISO/IEC 27018 No. 12.4**<br>- **ISO/IEC 27002 No. 12.4** |

## TCDP No. 25 – Job control

*Requirement*

The controls of ISO/IEC 27018 Nos. A.5, A.10.11 and A.10.12 as well as A.2.1 shall be normative as obligatory requirements.

*Implementation recommendation*

In implementation, account must be taken of the need for job control to comprise both the supervision of contractually agreed and other technical and organisational measures taken by the cloud service provider. The requirements of the cloud service user must also be included in the contracts of the cloud service provider with subcontractors. Independent agencies can assess the suitability of control measures for the contractual compliance of data processing (cf. ISO/IEC 27018 No. 18.2.1).

| Security category | Implementation recommendations |
|---|---|
| | - **ISO/IEC 27018 No. A.2.1**<br>- **ISO/IEC 27018 No. A.5.1**<br>- **ISO/IEC 27018 No. A.5.2**<br><br>**General organisational measures**<br>- Documentation of systems, procedures and processes applied for the respective cloud service (software, hardware, organisational units involved, roles and service providers)<br>- Exact description of all technical and organisational measures taken<br>- Procedure for in-house verification of adherence to technical and organisational measures<br>- Setting up (and documenting) a procedure for verifying adherence to measures for the following:<br>o Appointment of a data protection officer (TCDP No. 5)<br>o Verification of compliance with the requirements for engaging subcontractors to TCDP No. 4<br>o Verification of the obligation of cloud service provider personnel to observe data confidentiality to TCDP No. 10<br><br>**Measures for carrying out instructions**<br>- Introduction and documentation of a procedure for ensuring that personally identifiable data processed under contract can only be processed in keeping with the instructions of the client, particularly:<br>- Procedure for the receipt, execution and documentation of individual instructions of the client<br>- Authentication of the identity of the client and its personnel and their representative authorisation for assigning jobs and issuing instructions and for the delivery and receipt of data and documents<br>- Adherence to the obligation to raise an objection (TCDP No. 3)<br>- Adherence to the obligation to report data protection breaches (TCDP No. 7)<br><br>**Measures for contracted processing**<br>- Informative documentation of the cloud service on the delimitation of the legal data protection responsibilities of the client and processor<br>- Provision of information for a procedural overview pursuant to Section 4g(2) of BDSG |

| | |
|---|---|
| | - Measures for ensuring the following:<br>o Correction, blockage and deletion of data (TCDP No. 6)<br>o Return of data to client (TCDP No. 9)<br>o Procedures for the deletion of remaining data during and in particular on completion of the outsourced data processing relationship (TDP No. 9)<br>o Recording data processing operations (access for reading and alteration) on an adequate scale to meet data protection needs and storage of these protocols for an appropriate period<br>o In-house controls when needed |
| II | - Procedure for reporting data protection events to the client for supporting compliance with the obligation under Section 42a of BDSG<br>- Obligation to take out insurance policies<br>- Agreement of contractual penalties for breaches of instructions<br>- Appropriate protection of protocol integrity<br>- Logging configuration changes<br>- Documentation of processes of change<br>- Regular in-house initiated controls of client data handling in keeping with instructions |
| III | - Enhanced integrity protection of protocols (e.g. by using separate protocol servers)<br>- Automated monitoring of alterations<br>- Increasing intensity of control by qualified experts |

Trusted Cloud

## TCDP No. 26 – Data availability

*Requirement*

The controls of ISO/IEC 27018 No. 12.3 and ISO/IEC 27002 Nos. 11.1.4, 11.2.1, 11.2.2, 11.2.4, 12.1., 12.2, 12.3, 12.6 and 12.7 shall be normative as obligatory requirements.

*Implementation recommendation*

| Security category | Implementation recommendations |
|---|---|
| I | - **ISO/IEC 27018 No. 12.3**<br>- **ISO/IEC 27002 No. 12.1.4**<br>- **ISO/IEC 27002 No. 11.2.2**<br>- **ISO/IEC 27002 No. 11.2.4**<br>- **ISO/IEC 27002 No. 12.1.3**<br>- **ISO/IEC 27002 No. 12.1.4**<br>- **ISO/IEC 27002 No. 12.2**<br>- **ISO/IEC 27002 No. 12.3**<br>- **ISO/IEC 27002 No. 12.6**<br>- **ISO/IEC 27002 No. 12.3** |
| II, III | - **ISO/IEC 27002 No. 11.1.4**<br>- **ISO/IEC 27002 No. 12.1.1**<br>- **ISO/IEC 27002 No. 12.1.2** |

## TCDP No. 27 - Separate processing

*Requirement*

Depending on the type of personally identifiable data or the data categories for protection, appropriate measures shall be taken to ensure that data collected for different purposes can be processed separately.

*Implementation recommendation*

| Security category | Implementation recommendations |
|---|---|
| I | - Client separation through business logic of application software |
| II | - Cryptographic client separation<br>- Separation of different users of a client in the business logic of application software |
| III | - Cryptographic separation of different fields of work of the same client for data collected for different purposes |

## TCDP No. 28 - Cryptography

*Requirement*

Where the cloud service provider applies cryptographic methods, ISO/IEC 27018 No. 10 and ISO/IEC 27002 No. 10 shall be normative as obligatory requirements.

*Implementation recommendation*

| **Security category** | **Implementation recommendations** |
|---|---|
| I, II, III | - **ISO/IEC 27018 No. 10**<br>- **ISO/IEC 27002 No. 10** |

## V. References


[i] On the working party, Legal Framework for Cloud Computing, see http://www.trusted-cloud.de/560.php.

[ii] Proposition paper, Legal Data Protection Solutions for Cloud Computing, available at http://www.trusted-cloud.de/369.php.

[iii] Working paper, Modular Certification of Cloud Services, available at http://www.trusted-cloud.de/369.php.

[iv] Proposition paper, Basic Principles of a Certification Procedure for Cloud Services, available at http://www.trusted-cloud.de/369.php.

[v] ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

[vi] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.

[vii] ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.

[viii] Working paper, Security Categories in Data Protection Certification, available at http://www.trusted-cloud.de/369.php.


**Publishing details**

**Published by**
Trusted Cloud Competence Centre
Pilot project, Data Protection Certification for Cloud Services
E-Mail: kompetenzzentrum@trusted-cloud.de
**www.trusted-cloud.de**

On behalf of the Federal Ministry for Economic Affairs and Energy

As at: April 2015