Trusted Cloud
Pilotprojekt Datenschutz-Zertifizierung für Cloud-Dienste

Trusted Cloud – Data Protection Profile for Cloud Services (TCDP) – Version 1.0

Publisher: Pilot project "Data Protection Certification for Cloud Services"
E-mail: info@tcdp.de; www.tcdp.de
Commissioned by the Federal Ministry for Economic Affairs and Energy
Date of publication: September 2016

Table of Contents

I. The TCDP and its Goals

The Trusted Cloud Data Protection Profile ("TCDP") is a set of auditing standards for the data protection certification of cloud services.

1. Addressees and function of the TCDP

Data protection certification enables providers of IT services to prove that their IT services meet the requirements of data protection law. Users of such certified IT services can be certain that these services conform to data protection requirements. Data protection certification pursuant to the TCDP applies to those cases where the collecting, processing, or using of personal data has been contracted out (outsourced data processing). Users of such services–as customers within the meaning of Section 11 of the [German] Federal Data Protection Act (BDSG)–must assure themselves that the contractors are complying with the requirements of the law. Obtaining such assurance is far easier if the provider of the IT service–as a contractor–can produce a certificate that confirms that its particular IT services satisfy the requirements of the law. And because cloud services are often provided as standardized services for a large number of users, data protection certification is especially important as it provides an efficient way for users to fulfil their statutory obligation to review such services.

The TCDP delineates the requirements that data protection law imposes on contractors (cloud service providers). It does not deal with the requirements that data protection law imposes on customers (cloud service users).

2. The TCDP and the statutory regulation of data protection certification

The TCDP is closely linked to the ultimate goal of bringing data protection certification under statutory regulation. The basis of the TCDP is the concept of data protection certification of cloud services that was developed by the working group "Legal Framework for Cloud Computing"[1] as part of the impact study of the programme "Trusted Cloud".[2] In the pilot project "Data Protection Certification", additional bases for certification under data protection law were developed. The TCDP is suitable for modular certification as presented in the paper "Modular Certification of Cloud Services".[3] It is also suitable for certification pursuant to the principles described in the paper "Cornerstones of a Certification Procedure for Cloud Services" [4] of the pilot project "Data Protection Certification for Cloud Services".

The TCDP is based on the [German] Federal Data Protection Act (BDSG). It implements the statutory requirements imposed by the BDSG on outsourced data processing and translates these into concretely verifiable norms. It is founded on the ISO/IEC standard 27018[5], which extends the internationally accepted ISO/IEC standards 27001[6] and 27002[7] to include requirements specific to clouds and particularly specific to data protection, and also incorporates the standard ISO/IEC 27017.[8]

ISO/IEC 27018, ISO/IEC 27017, and ISO/IEC 27002 are incorporated by way of reference in the TCDP to the extent to which they are capable of concretizing the statutory requirements of the BDSG. The TCDP modifies and supplements the ISO/IEC standards to the extent required to fulfil the statutory requirements of the BDSG. Therefore the benchmark and the model for the TCDP are the statutory requirements imposed by the BDSG on outsourced data processing.

3. Creation and application of the TCDP

The TCDP was developed in the pilot project "Data Protection Certification for Cloud Services", a project of the Federal Ministry for Economic Affairs and Energy. The pilot project was carried out in two phases. The first one was from November 2013 to April 2015 and the second from September 2015 to September 2016. The project participants included public authorities responsible for data protection supervision, business enterprises as cloud service providers, law firms, public auditors (accountants), testing companies, business associations, the foundation Stiftung Datenschutz, the German standardization organization DIN e.V., and various academics/scientists. The Federal Ministry of the Interior and the Federal Office for Information Security, as well as the EU Commission in the first phase, played the role of observers.[9]

The TCDP was released in April 2015 as "beta version" TCDP 0.9. It has undergone testing and further developments through test (pilot) certifications since September 2015. The TCDP was released as a full version 1.0 in September 2016.

In order to ensure that the auditing and certification pursuant to the TCDP are carried out properly, the "Rules of Procedure for Certification According to the Trusted Cloud Data Protection Profile for Cloud Services (TCDP)" was developed in the pilot project "Data Protection Certification for Cloud Services". The Rules of Procedure were published together with TCDP 1.0 in September 2016. TCDP certifications are only to be granted on the basis of the provisions of these Rules of Procedure. The certificate symbol for TCDP certifications may only be displayed in compliance with Rules of Procedure.

The administration and further development of the TCDP–as a set of auditing standards for cloud services on the basis of the BDSG–and of the Rules of Procedure for TCDP Certification were transferred to the German foundation Stiftung Datenschutz. The administrator also provides an information centre for TCDP certification.

4. General Data Protection Regulation and European Data Protection Certification

The TCDP is rooted in the goal of a legally regulated European data protection certification. The TCDP is meant to foster the development of a European data protection certification by developing the bases on which data protection certification can be modelled. The General Data Protection Regulation (Regulation (EU) 2016/679) contains the central principles of a

statutory framework for data protection certification. The pilot project strongly advocates the development of a TCDP-like certification on the basis of Regulation (EU) 2016/679. The underlying idea is that TCDP certifications–after auditing standards and certification procedures have been created–will be converted into certifications pursuant to the General Data Protection Regulation for cloud services, as provided for in the Code of Practice for TCDP Certification.

II. Structure and Use of the TCDP

1. The text categories of the TCDP

Similar to the ISO/IEC 27000 series of standards and other standards, the TCDP draws a distinction between "requirements" and "implementation guidance" and contains additional "explanatory notes".

The "requirements" are those normative conditions that must be fulfilled in order to obtain certification on the basis of the TCDP. In other words, they are auditing requirements. Wherever TCDP requirements describe control mechanisms of ISO/IEC 27018, ISO/IEC 27017, or ISO/IEC 27002 as "compulsory", such controls become requirements of the TCDP and must therefore be fulfilled.

Because the requirements of the BDSG are all obligatory requirements, the TCDP standards are usually worded as obligatory requirements as well. But because the wording of the ISO/IEC 27018 and ISO/IEC 27002 requirements is primarily of a non-compulsory nature ("should"), any references made by the TCDP to ISO/IEC standards must be changed into obligatory requirements. In this respect the TCDP takes two different approaches. Some TCDP standards refer to ISO/IEC standards and make it explicitly clear that these are compulsory requirements, i.e. that these are to be read as "shall" [must] and not as "should". Sometimes the TCDP uses its own wording for a particular requirement and refers in square brackets to the corresponding ISO/IEC controls. In a few cases it is also unclear whether the ISO/IEC standard is compatible at all with the requirements of the BDSG, or the compatibility is at least not obvious from the wording of it. The original wording of the requirement and the reference to the ISO/IEC standard in brackets make it clear that, in the case of a conflict, the BDSG-oriented requirement of the TCDP is decisive.

The implementation guidance provisions are meant to guide and assist in the understanding and implementing of the requirements; they are not themselves "normative" requirements.

The implementation guidance provisions to the individual TCDP standards are geared to the protection categories as laid down in the TCDP Concept of Categories of Protection Needs.[10] Where a TCDP standard does not contain such a division into protection categories, the implementation guidance applies equally to all protection categories.

The implementation guidance incorporates, where appropriate, the implementation recommendations of the ISO standards by reference to them. The same applies in this respect as in the case of the requirements.

The "explanatory notes" are meant to facilitate a better understanding of the requirements and where they derive from in the law.

2. The use and way of citing ISO/IEC standards

Because the TCDP makes references to ISO/IEC 27018 and ISO/IEC 27002 and to ISO/IEC 27017, it presupposes knowledge of these standards. A preceding certification pursuant to ISO/IEC 27001 is not a prerequisite of the TCDP. The use by the TCDP of the same system and terminology of the ISO/IEC 27000 series makes a certification pursuant to TCDP considerably easier if such a certification already exists.

The ISO/IEC standards are cited in their most current versions (ISO/IEC 27018:2014, ISO/IEC 27002:2013, ISO/IEC 27017:2015). For an easier reading of the TCDP, the standards are referred to in the text in their abbreviated forms: “ISO/IEC 27018”, “ISO/IEC 27002”, and “ISO/IEC 27017”.

ISO/IEC 27018 and ISO/IEC 27017 are based on ISO/IEC 27001 and ISO/IEC 27002 and make frequent references to the controls and implementation guidance provisions of ISO/IEC 27002 without making any independent assertions. In these cases, the TCDP refers exclusively to the controls and the implementation guidance provisions of ISO/IEC 27002. Wherever ISO/IEC 27018 and ISO/IEC 27017 contain supplementary assertions, the TCDP also refers to ISO/IEC 27018 and ISO/IEC 27017.

III. Protection Categories

1. The Concept of Categories of Protection Needs

The TCDP is based on the Concept of Categories of Protection Needs. It was developed in the pilot project "Data Protection Certification for Cloud Services" and was first described in the working paper "Protection Categories in Data Protection Certification" in April 2015.[11] The Concept of Categories of Protection Needs was published in an updated form as TCDP Concept of Categories of Protection Needs 1.0 in September 2016.[12]

The aim of the Concept of Categories of Protection Needs is to simplify the individual standards of the law – the requirements imposed on the technical and organizational measures are determined by the protection needs of the particular data processing activity – by classifying them in protection categories. The protection categories therefore have a double function: They define on the one hand the protection needs of the data processing activities and on the other hand the requirements imposed on the technical and organizational measures. In order to clearly distinguish between these two functions, the Concept of Categories of Protection Needs distinguishes between categories of protection needs and categories of protection requirements.

The categories of protection needs define the protection needs of data processing activities on the basis of general factors. These include the type of data and the circumstances of the concrete data processing activity.

The categories of protection requirements define in a general way the technical and organizational requirements applicable to the data processing services of the particular category. Thus for every category of protection needs there is a corresponding category of protection requirements.

Which exact category of protection (requirements) a certified cloud service provider is in is stated in the TCDP certificate.

2. Responsibilities of the cloud service user and the cloud service provider

The distinction drawn between categories of protection needs and categories of protection requirements corresponds to the roles and responsibilities of the cloud service user and the cloud service provider where there is outsourced data processing.

The cloud service provider is responsible for categorizing its services in one of the categories of protection requirements and for ensuring that its services satisfy the requirements of this category of protection requirements at all times.

In the certification process, the certifying body classifies the particular service in one of the categories of protection (requirements) on the basis of the audit made and the concrete technical and organizational measures. In the certificate itself, the service's suitability for a concrete category of protection (requirements) is stated.

The cloud service user–as the responsible entity and as the customer–has the task of determining the protection needs of its data processing. It is therefore the cloud service user's responsibility to ascertain which category of protection requirements applies to its data processing activity and to choose a cloud service for its data processing that at least satisfies the requirements of this category. The ascertainment of the protection needs of a data processing activity is described in detail in the TCDP Concept of Categories of Protection Needs.

3. The protection categories of the TCDP

The TCDP distinguishes between three protection categories (I, II, III), each of which contains a definition of what protection is needed (categories of protection needs) and what protection is required (categories of protection requirements).

Two other categories of protection needs are also defined. The function of these, however, is rather to provide assistance in distinguishing them from the other categories. One of these is protection category 0, which indicates an absence of a need for protection under data protection law. This concerns such things as data with no references to a person. The other is protection category III+, which indicates a need for protection that does not fit one of the definitions of the protection categories and therefore no certification is available for this. This concerns such things as data processing activities with extremely high protection needs and very individual circumstances. And because no certification can be granted pursuant to protection categories 0 and III+, no categories of protection requirements are defined for them.

a) Categories of protection needs

Category of protection needs 0

Data processing activities (i.e. the service requested from the cloud service) that do not contain, produce, or sustain information or protection-meriting information about the personal affairs of natural persons or that do not enable any such thing.

Category of protection needs 1

Data processing activities that through the data involved and the concrete collection, processing, or use of this data contain, produce, or sustain information about the personal affairs of natural persons (data subject/s) or that enable any such thing. Experience shows that the unauthorized processing or use of this data usually does not result in any concrete disadvantages for the data subjects (interference with legally protected interests) or these can be easily prevented or brought to an end by the data subject.

Category of protection needs 2

Data processing activities that on the basis of the data used or the concrete collection, processing, or use of such data are capable of providing or sustaining information about the personality or the life of the data subject or that could lead to such or that are otherwise of significance to the data subject's affairs. Experience shows that the unauthorized processing or use of this data can result in concrete disadvantages for the data subjects.

Category of protection needs 3

Data processing activities that on the basis of the data used or the concrete collection, processing, or use of such data are substantially capable of providing or sustaining information about the personality or the life of the data subject or that could lead to such or that are otherwise of major significance to the data subject's affairs. The unauthorized collection, processing, or use of this data can result in serious disadvantages for the data subjects.

b) Categories of protection requirements

Category of protection requirements 1

The cloud service provider must ensure through risk-appropriate technical and organizational measures that the data is not being processed or used without authorization.

The measures must be capable, in the normal case, of preventing such occurrences resulting from the technical or organizational errors, including the operating errors, of the cloud service provider or its employees or from the negligent acts of third parties. A minimum amount of protection must be provided to make intentional intrusions more difficult to achieve.

Category of protection requirements 2

The cloud service provider must ensure through risk-appropriate technical and organizational measures that the data is not being processed or used without authorization.

The measures must be capable, in the normal case, of preventing such occurrences resulting from the technical or organizational errors, including the operating errors, of the cloud service provider or its employees or from the negligent acts of third parties. These measures must also be capable, in the normal case, of preventing damage caused by the negligent acts of authorized persons. Adequately secure protection must be provided in order to prevent expectable kinds of intentional intrusions. This especially includes adequate protection against known attack scenarios and measures through which the intrusions in the normal case can be identified (subsequently).

Category of protection requirements 3

The cloud service provider must ensure through risk-appropriate technical and organizational measures that the data is not being processed or used without authorization.

The measures must be capable of adequately preventing such occurrences resulting from technical or organizational errors, including operating errors, or from negligent or intentional acts. This especially includes adequate protection against known attack scenarios and processes for identifying abuses. Each intrusion must be subsequently identifiable.

4. Ascertaining the category of protection needs

It is the cloud service user's responsibility to ascertain the protection needed (see point 2 above). The protection needed is ascertained in a three-step process:

- Step 1: The abstract protection needs of the data to be processed are determined according to the type of data (examples are found in Chapter 3.2 of the Trusted Cloud Concept of Categories of Protection Needs).
- Step 2: A review is made to determine whether the protection needs are higher in light of the concrete application.
- Step 3: A review is made to determine whether the protection needs are lower in light of the concrete circumstances.

The protection needs of the concrete data processing activity are then classified in one of the aforementioned categories of protection needs. A detailed description of this process with examples of the data types/application contexts is found in Chapter 3.2 of the Trusted Cloud Concept of Categories of Protection Needs.

IV. Table of Standards

BDSG	Subject Matter of the Standard	Short Description	TCDP-No.
Section 11	Contractual requirements	Fulfilling the statutory requirements imposed on the contract	1
Section 11(2)	Provision of services on the basis of a contract	Provision of services only per a contract for outsourcing data processing	1.1.
Section 11(2) sent. 2	Form of the contract	Contract must be in written form	1.2.
Section 11(2) sent. 2 no. 1	Objects and duration of the subcontracting	Objects and duration of the subcontract must be stipulated	1.3.
Section 11(2) sent. 2 no. 2	Scope/type/purpose/group of data subjects	Scope/type/purpose of collection, processing, use and the group of data subjects must be stipulated.	1.4.
Section 11(2) sent. 2 no. 3	Technical and organizational measures	Measures required by Section 9 BDSG must be stipulated	1.5.
Section 11(2) sent. 2 no. 4	Correcting/deleting/blocking	Requirements for correcting, deleting, and blocking data on the contractor's instructions must be stipulated	1.6.
Section 11(2) sent. 2 no. 5	Contractor's obligations	Contractor's obligations, especially controls, must be stipulated	1.7.
Section 11(2) sent. 2 no. 6	Subcontractor	Whether the contractor is allowed to subcontract must be stipulated	1.8.
Section 11(2) sent. 2 no. 7	Customer's rights and contractor's obligations	Customer's controlling rights and contractor's duties to acquiesce and cooperate must be stipulated	1.9.
Section 11(2) sent. 2 no. 8	Reporting infringements	Which infringements of law or contractual agreements that must be reported must be stipulated	1.10.
Section 11(2) sent. 2 no. 9	Customer's powers of instruction	Customer's powers to instruct the contractor must be stipulated	1.11.
Section 11(2) sent. 2 no. 10	Duty to return	Return of data media and deletion of data by the contractor must be stipulated	1.12.
Sections 11 and 5	Relationship between cloud service provider and cloud service user	Organizational precautions to be taken by the contractor regarding conformity of services to data protection law.	
Section 11(3) sent. 1	Customer's instructions are binding	No collecting/processing/using of data outside the customer's instructions	2

BDSG	Subject Matter of the Standard	Short Description	TCDP-No.
Section 11(3) sent. 2	Reporting duty	Contractor's duty to report when customer's instructions infringe the BDSG or other data protection laws	3
Section 11(2) sent. 1	Subcontractor (substantive)	Contractor must prove that subcontractors were chosen properly	4
Section 11(4)	Company data privacy officer	Contractor's obligations pursuant to Sections 5, 9, 43(1) nos. 2, 10, and 11, (2) nos. 1 to 3, and (3), Section 44, and Sections 4f, 4g, and 38 BDSG	5
Section 11	Correcting, blocking, and deleting data	The correcting, blocking, and deleting of data must be made possible	6
Section 11	Reporting duty	Infringements of statutory or contractual provisions must be reported	7
Section 11(2) sent. 2	Customer's controlling rights / contractor's duties to acquiesce and cooperate	Contractor must have processes for customer audits	9
Section 11(2) sent. 2 no. 10	Duty to return	Contractor must prove that it has a return process	10
Section 5	Data privacy	Contractor must put employees under a duty of data privacy	11
Section 9 in conjunction with the Annex	Technical and organizational security of the cloud service		
Sent. 2 no. 1 of Annex to Section 9	Physical access controls	Stopping unauthorized persons from physically accessing processing facilities	22
Sent. 2 no. 2 of Annex to Section 9	Physical access controls	Preventing unauthorized persons from accessing data processing systems	23
Sent. 2 no. 3 of Annex to Section 9	Access controls	Warranting that entitled persons can only access their own data area	23
Sent. 2 no. 4 of Annex to Section 9	Transmission controls	Protection of data during transportation, storage, and transmission against unauthorized access	24
Sent. 2 no. 5 of Annex to Section 9	Data-entry controls	Warranting that users who enter, alter, or delete personal data are subsequently identifiable	25

BDSG	Subject Matter of the Standard	Short Description	TCDP-No.
Sent. 2 no. 6 of Annex to Section 9	Instruction control	Warranting that personal data can only be processed pursuant to contractor's instructions	26
Sent. 2 no. 7 of Annex to Section 9	Availability control	Warranting that personal data cannot be accidentally destroyed or lost	31
Sent. 2 no. 8 of Annex to Section 9	Separate processing	Warranting that data collected for different purposes can be processed separately according to its particular purpose	27
Section 9	Cryptography	Requirements imposed on use of cryptographic processes	28

V. Requirements and Implementation Recommendations

1. Contractual regulation of outsourced data processing

TCDP No. 1 – Contractual basis

Explanatory notes

The cloud service provider must endeavour to ensure that its services for the cloud service user are being performed pursuant to a contract (cloud contract) that satisfies the statutory requirements imposed by the BDSG on outsourced data processing. The requirements set out below are intended to ensure the attainment of this goal.

Nos. 1.3 to 1.12 of the TCDP can be satisfied by the cloud service provider through the use of a contract that fulfils the referred to requirements and through the taking of organizational precautions to ensure that the cloud service is only being performed on the basis of such a cloud contract. Standard form contracts could be useful in the creation of such contracts.

TCDP Nr. 1.1 – Performing services on the basis of a contract

Requirements

The cloud service provider must ensure through suitable organizational precautions that the cloud services are only being performed once a contract that satisfies the requirements of TCDP No. 1 has been concluded with the cloud service user.

TCDP No. 1.2 – Form of the contract

Requirements

The cloud service provider must offer to conclude a written contract for the outsourcing of data processing.

Implementation guidance

The cloud service provider’s readiness to conclude a written contract could be evidenced through such things as a draft contract (standard form contract) and a process pursuant to which the contract is concluded in written form.

TCDP No. 1.3 – Objects and duration of the contract

Requirements

The objects and the duration of the contract must be stipulated in the cloud contract.

Implementation guidance

The contract should stipulate either a concrete period of time or should clearly state that it is being concluded for an indefinite period of time. Contracts concluded for indefinite periods of time should include provisions regulating the terminating of the contract, especially the required notice periods for such terminations.

These things can be warranted by the cloud service provider through the use of a draft contract (standard form contract) that contains these provisions and through adherence to a procedure pursuant to which a contract containing these provisions is concluded.

TCDP No. 1.4 – Type and purpose of the data processing

Requirements

The cloud contract must stipulate the scope, the type, and the purpose of the planned collection, processing, or use of data, the type of data, and the group of the data subjects.

Implementation guidance

Although this detailed information does not have to cover every single concrete case, it should be stated so precisely that the data usage permitted by the outsourced data processing service is clearly identifiable.

This can be achieved in different ways depending on the type of cloud service. Particularly in the case of standard SaaS services where the type and purpose of the data processing is apparent from the purpose of the program itself, a simple reference to the program description in the documentation will suffice. But in the case of more complex or less standardized services (e.g. PaaS), an agreement with the cloud service user is usually required. One way of doing this would be through the use of an electronic form in which the cloud service user enters the information required.

TCDP No. 1.5 – Technical and organizational measures, location of the data processing activities

Requirements

(1) The technical and organizational measures required by TCDP Nos. 22–28 must be stipulated in the cloud contract.

(2) The cloud service provider must state which protection category is warranted by it.

The cloud contract must specify the countries in which the cloud service user's data is being processed, especially where it is being stored.

Implementation guidance

The above requirements can be stipulated in a schedule to the contract. The information in relation to the implementation of TCDP Nos. 22–28 (Section 9 BDSG and its Annex) could be expressed as security goals, while the concrete measures used for achieving such goals could be left to the cloud service provider. The stipulating of these matters should be in the form of a security concept (TCDP No. 21) and attached to the contract as a schedule.

For the cloud service user it is important to know which category of protection requirements– pursuant to the Trusted Cloud Concept of Categories of Protection Needs–the cloud service provider is in. It is therefore advisable in the cloud contract to include an express provision that warrants a specific protection category pursuant to the Trusted Cloud Concept of Categories of Protection Needs.

TCDP No. 1.6 – Correcting, deleting, and blocking data

Requirements

The process for correcting, deleting, and blocking data (TCDP No. 6) must be stipulated in the cloud contract.

Implementation guidance

It is advisable to clearly state the deletion deadlines and the deletion procedures.

TCDP No. 1.7 – Obligations of the cloud service provider

Requirements

In the cloud contract, the cloud service provider's data protection obligations pursuant to Section 11(4) BDSG must be stipulated as contractual obligations owed by the cloud service provider to the cloud service user.

Explanatory notes

According to Section 11(2) sent. 2 no. 5 BDSG, the cloud contract must clearly state which of the statutory obligations set out there are owed by the cloud service provider as a contractor.

Implementation guidance

It suffices if the statutory provisions applicable to the cloud service provider are stated in the cloud contract. It is common practice and it makes good sense to not simply cite the section numbers of these but to also describe the contents of them or reproduce their exact wording.

TCDP No. 1.8 – Subcontractors

Requirements

(1) The right to create subcontractual relationships must be stipulated in the cloud contract.

(2) In the cloud contract, the cloud service provider must undertake as towards the cloud service user to comply with the requirements laid down in TCDP No. 4 when contracting with subcontractors.

Explanatory notes

Subcontractors may only be engaged with the cloud service user's consent. What is required is a general consent to engage subcontractors. A specific consent to engage a specific subcontractor is not required. However, the cloud service provider must inform the cloud service user of the identity of all subcontractors (No. 4.2).

TCDP No. 1.9 – Cloud service user's control rights

Requirements

The cloud service user's control rights (TCDP No. 9) and the cloud service provider's corresponding duties to acquiesce in and cooperate with these must be stipulated in the cloud contract.

TCDP No. 1.10 – Reporting of infringements and demands for data disclosures

Requirements

(1) The cloud contract must stipulate which infringements of the cloud service provider or the persons employed by it (see TCDP No. 7) of the statutory provisions on the protection of personal data or of the contractual agreements have to be reported.

(2) The cloud contract must stipulate that the cloud service provider must inform the cloud service user promptly of any demands for data disclosures if the informing of the cloud service user is lawful (see TCDP No. 8).

Implementation guidance

As a minimum requirement, the cloud contract must contain an obligation to promptly inform [the cloud service user] of any infringements of data protection law and of demands for disclosures of data. It is advisable to also stipulate in the contract in which form and via which communication routes the information has to be given.

TCDP No. 1.11 – Cloud service user's powers of instruction

Requirements

The cloud contract must stipulate the scope of the powers of instruction retained by the cloud service user vis-à-vis the cloud service provider (TCDP No. 2).

Implementation guidance

The right to issue individual instructions must be reserved for the cloud service user. It is advisable to stipulate in the contract that the right to issue individual instructions must be made in text form and must be confirmed by the cloud service provider. The contract should be very precise about which persons are authorized to issue individual instructions. The actual names of the persons authorized to issue individual instructions could be included in the cloud contract.

TCDP No. 1.12 – Returning and deleting data

Requirements

The cloud contract must stipulate the obligations of the cloud service provider to return and delete data (TCDP No. 10).

Implementation guidance

The cloud contract should at least contain the obligations set out in TCDP No. 10. It would be advisable, however, to provide for this in more detail. One way of doing this would be to refer to the relevant principles of the cloud service provider.

2. Relationship between cloud service providers and cloud service users

TCDP No. 2 – Instructions are binding on the cloud service provider

Requirements

The cloud service provider must ensure through suitable measures that when executing its services it is obligated to collect, process, and use the data only within the scope of the instructions of the cloud service user.

Explanatory notes

There are three places in the BDSG (Section 11(2) sent. 2 no. 9, (3) sent. 1, Annex to Section 9 no. 4 BDSG) that address the fact that the cloud service provider is bound by the instructions [of the cloud service user]. This is why the TCDP also refers in three places to this binding obligation: TCDP No. 2 states that the cloud service provider must undertake to follow the instructions, TCDP No. 1.11 says that this is a required component of the cloud contract, and TCDP No. 26 obligates the cloud service provider to ensure through technical and organizational measures that such instructions are being followed.

Implementation guidance

The cloud service provider should ensure through an organizational process that the contract contains an undertaking of the cloud service provider vis-à-vis the cloud service user to execute the outsourced data processing activity exclusively in accordance with the instructions of the cloud service user. This could be done by using a suitable standard form contract (see TCDP No. 1.11). In addition, the technical or organizational system of the cloud service provider should be set up in such a way that a cloud service cannot be executed if such an undertaking is missing.

The instructions must define the data processing to be performed by the cloud service provider. This can be achieved by an agreement on the functionalities of the cloud service. This agreement could be included in the cloud contract, for example through a reference to the documentation of the functionalities (see TCDP No. 1.11).

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

TCDP No. 3 – Duty to remonstrate

Requirements

The cloud service provider must ensure through suitable measures that it will inform the cloud service user promptly if it is of the opinion that an instruction issued by the cloud service user

infringes data protection law and that it will wait for the cloud service user's decision before acting on the instruction.

Explanatory notes

According to the principles of outsourced data processing, the cloud service user is responsible for ensuring that the data processing activity conforms to data protection law, which is why the cloud service user also has the right to issue instructions to the cloud service provider. Nevertheless, the cloud service provider may not blindly execute an instruction whose lawfulness it doubts. Instead, Section 11(3) sent. 2 BDSG imposes a duty on the cloud service provider to remonstrate in such cases. It has to warn the cloud service user if it has doubts about the compatibility of the instruction with the effective data protection laws and must wait for the cloud service user's decision.

Implementation guidance

The cloud service provider can provide and document a procedure pursuant to which any instructions whose compatibility with data protection law is doubtful can be submitted to the cloud service user for the cloud service user's decision prior to execution. It is advisable to stipulate that the cloud service user must make an express decision in text form. This should be contained in the cloud contract, if applicable.

TCDP No. 4 – Subcontractors

Explanatory notes

Cloud services are often performed by cloud service providers through the use of suppliers, which are integrated as subcontractors in the outsourced data processing activities. And because subcontractors themselves also frequently use subcontractors, there are often multiple levels of subcontracting relationships.

Although the use of subcontractors and sub-subcontractors is generally permitted, the cloud service provider–as a contractor–must ensure that the requirements imposed on outsourced data processing are being complied with by all subcontractors at all levels.

TCDP No. 4.1 – Basis for engaging subcontractors

Requirements

The cloud service provider must ensure that a cloud service carried out by a subcontractor is only performed for a cloud service user if and to the extent to which the cloud service user has consented to it.

Implementation guidance

The cloud service provider that engages subcontractors could satisfy this requirement through a procedure that only allows the executing of the service for the cloud service user if a review has been made to determine whether such consent exists, which as a rule is achieved through the concluding of a cloud contract that contains just such a provision (see TCDP No. 1.8).

TCDP No. 4.2 – Informing the cloud service user

Requirements

(1) The cloud service provider must inform the cloud service user of the identity of all of the subcontractors engaged by it (including the addresses at which they can be summoned/served by a court).

(2) The cloud service provider must inform the cloud service user of the identity of all of the sub-subcontractors (including the addresses at which they can be summoned/served by a court) used by the subcontractors of the cloud service provider. The same applies to all levels of subcontracting.

(3) The cloud service provider must inform the cloud service user of all changes to the identity of subcontractors or sub-subcontractors, especially all newly added subcontractors or sub-subcontractors.

Implementation guidance

The information can be provided electronically, for example via a link on a (protected) area of the website that contains the information. The information regarding changes can be sent for example by e-mail or in another electronic way.

TCDP No. 4.3 – Contractual basis of the subcontracting

Requirements

(1) The cloud service provider must ensure that its subcontractors are not acting without a valid contract for the sub-outsourcing of data processing.

(2) The cloud service provider must put its subcontractors under an obligation to ensure that their sub-subcontractors are not acting without a valid contract for the sub-outsourcing of data processing and an obligation to impose the same obligation on their sub-subcontractors.

Implementation guidance

The cloud service provider can satisfy the requirement in (1) above through a procedure that only allows the use of a subcontractor to perform a service if the contract for the sub-outsourcing of data processing between the cloud service provider and the subcontractor has been reviewed.

The requirement in (2) can be satisfied for example by including this obligation in the contract for the sub-outsourcing of data processing.

TCDP No. 4.4 – Selection and control of the subcontractor

Requirements

(1) The cloud service provider must ensure that it is only engaging subcontractors that can warrant that the services to be performed by them comply with the data protection law requirements applicable to such services.
(2) The cloud service provider must satisfy itself that its subcontractors fulfil the data law requirements applicable to the services to be performed by them.
(3) The requirements pursuant to (1) and (2) apply analogously to subcontractors at all levels with respect to the sub-subcontractors engaged by them.

Implementation guidance

The cloud service provider could fulfil the requirements of (1) and (2) by checking the (valid) certification [of the subcontractor] in order to satisfy itself that the subcontractor (still) meets the requirements.

If the cloud service provider cannot rely on the certifications of its subcontractors, then it is obligated to satisfy itself that the subcontractors really are complying with the requirements of data protection law. In this respect, the implementation guidance provisions of ISO/IEC 27017 points 15.1.2 and 15.1.3 and ISO/IEC 27002 point 15 are to be understood as non-compulsory guidelines.

TCDP No. 4.5 – Instructions of the cloud service user

Requirements

(1) The cloud service provider must ensure that the cloud service user's instructions are passed on to the subcontractors.
(2) The cloud service provider must put its subcontractors under an obligation to ensure that the instructions issued by the cloud service user are being followed and that they put their sub-subcontractors under the same obligation.

(3) The cloud service provider must assure itself that the cloud service user's instructions are being followed by the subcontractors and their sub-subcontractors at all levels.

Explanatory notes

If the instructions of the cloud service user are to be passed down along the "chain" of (sub-)subcontractors, the cloud service provider has an overall organizational responsibility to ensure that the cloud service user's instructions are being followed.

Implementation guidance

The cloud service provider can satisfy the requirement in (1) by establishing a procedure through which the cloud service user's instructions are passed on to the subcontractors, for example technically via an automatic process or manually via an organizational process of passing the instructions on.

The requirement in (2) can be satisfied for example by including this obligation in the contract for the sub-outsourcing of data processing. The cloud service provider can satisfy the requirement in (3) for example by using suitable measures (checking the certifications or carrying out its own review) to satisfy itself that the instructions are being passed on and followed.

TCDP No. 5 – Data protection officer and statutory requirements

Requirements

The cloud service provider must ensure through the use of suitable measures that the data protection law requirements of Sections 4f and 4g or Section 18 BDSG or of the provisions of other data protection acts of the German Länder are being fulfilled.

Explanatory notes

Section 11(4) BDSG imposes specific statutory requirements on the cloud service provider in its capacity as a contractor. Sections 9 and 11 BDSG referred to in it are being implemented through the remaining requirements of the TCDP. The provisions on the data protection officer (Sections 4f and 4g BDSG) or on compliance (Section 18 BDSG or the data protection acts of the German Länder) are implemented in TCDP No. 5, and the provisions on data privacy (Section 5 BDSG) are implemented in TCDP No. 11. Section 38 BDSG (public supervisory authority) or Sections 24–26 BDSG (Federal Commissioner for Data Protection and Information), or the corresponding provisions of the data protection acts of the German Länder, are only relevant to certification in relation to the referencing of them in the contract and are therefore implemented through TCDP No. 1.7. Sections 43 and 44 BDSG concern administrative and criminal offences and are therefore irrelevant to certification.

If the cloud service provider is obligated to appoint a data protection officer, then the cloud service provider must fulfil this obligation to make a valid appointment by ensuring that the

conditions required for the autonomy, reliability, and expertise of the data protection officer are being met. This presupposes that the appointing cloud service provider has made an advance review of the suitability of the prospective data protection officer in order to verify that the requirements regarding reliability (especially regarding possible conflicts of interest) and the necessary expertise in relation to the concrete needs of the appointing cloud service provider are satisfied by the prospective data protection officer. This requires the cooperation of the prospective data protection officer (self-assessment of his/her qualifications, information about the required expertise, conflicts of interest, etc.).

If the data protection officer is employed at another business enterprise (i.e. an external data protection officer of the cloud service provider) or is simultaneously the data protection officer at several business enterprises, then he/she must also be autonomous in relation to such employer or other customers.

Implementation guidance

Through the use of organizational measures in the form of a data protection system, the cloud service provider must ensure that the data protection officer is able to exercise his/her tasks autonomously and in accordance with the law.

The cloud service provider must keep a written documentation of the systems, procedures, and processes used for each cloud service (software, hardware, organizational units involved, roles, and service providers) and an exact description of the technical and organizational measures as a whole (e.g. in a data security concept) and must allow the data protection officer and (upon request) the public supervisory authorities access to such documentation.

A valid appointment of a data protection officer (DPO) includes:

– the documentation of the suitability test by the DPO and the cloud service provider, especially regarding his/her expertise and reliability in relation to the type and scope of the data processing activity and any possible conflicts of interest;

– a written document containing the appointment signed by both parties;

– proof of the requisite autonomy of the DPO (if an external DPO has been appointed, then proof of his/her autonomy in relation to his/her employer may also be required);

– proof that the DPO has the resources needed to fulfil his/her tasks and is free of conflicts of interest; in the case of external DPOs, disclosure of the other positions he/she holds and the time resources needed for these (the time resources of the DPO must be appropriate to the protection needed and the number of customers [support may be needed in the form of data protection coordinators]; there should be a yearly plan and budgeted amounts allocated for the activities of the DPO [e.g. for engaging external experts and for keeping the DPO's knowledge up to date]);

– the direct accountability of the DPO to the executive officers of the cloud service provider.

The DPO and the officer for IT/information security must be appropriately incorporated in the organization of the cloud service provider. They are obligated to cooperate to a reasonable extent (provide each other with information and support).

The DPO must perform regular–e.g. quarter yearly–internal audits and must report on these to the management of the cloud service provider.

TCDP No. 6 – Correcting, deleting, and blocking data

Requirements

The cloud service provider must ensure through the taking of suitable measures that cloud service users can correct, block, and delete personal data themselves or can have it done by the cloud service provider [ISO/IEC 27018 point A.1.1.].

Explanatory notes

Section 11(2) sent. 2 no. 4 BDSG implies that customers must be able to correct, delete, or block personal data or at least be able to have these things done for them so that they can fulfil the obligations imposed on them by Section 35 BDSG. This requirement is essentially found in ISO/IEC 27018 point A.1.1., even though the blocking [of data] is not expressly referred to.

Implementation guidance

A procedure for enabling the customer to exercise the data subject's rights to correct, block, and delete data and to be informed [about certain things] must be established and documented. Areas of competence must be defined for this.

For cloud service users who are unable to exercise these data subject rights themselves, a contact point that is reasonably easy to reach and that has the power to quickly induce the implementing of these rights must be available to them.

The documentation of these cases (requests to implement the data subject rights) must be ensured.

TCDP No. 7 – Duty to report infringements of data protection

Requirements

The cloud service provider must ensure through suitable measures that the cloud service user is promptly informed of any infringements of statutory or contractual data protection requirements in cases where it cannot be ruled out that the transmission, obtaining of knowledge about, or the altering of personal data is unlawful.

Explanatory notes

Although TCDP No. 7 in terms of its subject matter is largely equivalent to ISO/IEC 27018 point A.9.1., it goes somewhat further on account of the statutory provision on which it is based. It demands that infringements also be reported when the unlawfulness of a transmission, an obtaining of knowledge about, or an altering of personal data–even though it has not been established–cannot be ruled out. The duty to report also includes the duty to report infringements committed by subcontractors and sub-subcontractors along the entire subcontracting "chain".

Implementation guidance

To ensure that the reporting is carried out promptly, certain persons must be designated responsible for deciding whether a reportable infringement exists and who is to report it to the cloud service user. The responsible parties must be reachable by the employees and subcontractors in a way that ensures that reports about (possible) infringements are received and processed in a swift manner.

What is generally needed to satisfy TCDP No. 7 is a management system for information security cases, i.e. a system to review the security cases to determine whether infringements of data protection law have occurred. The implementation guidance provisions of ISO/IEC 27018 point 16.1.1, ISO/IEC 27017 points 16.1.1 and 16.1.2, and ISO/IEC 27002 points 16.1.1 and 16.1.2 are to be understood as non-compulsory guidelines.

The reporting system chosen by the cloud service provider must be a system that enables cloud service users to fulfil any reporting duties pursuant to Section 42a BDSG or pursuant to other laws.

TCDP No. 8 – Duty to inform and document in cases of demands for data disclosure

Requirements

(1) The cloud service provider must promptly inform the cloud service user of any–for the cloud service provider–legally compulsory demands for disclosures of data if such informing of the cloud service user is permitted by law.

(2) The control provisions of ISO/IEC 27018 point A.5.2. must be understood as compulsory requirements.

Implementation guidance

The cloud service provider can provide and document a procedure for promptly reviewing demands for data disclosures (for example from the criminal prosecution authorities) to determine whether it is lawful to inform the cloud service user about them and, if it is lawful, to inform the cloud service user without undue delay.

The implementation guidance provisions of ISO/IEC 27018 point A.5.2. are to be understood as non-compulsory guidelines.

TCDP No. 9 – Control rights of the cloud service user

Requirements

The cloud service provider must ensure through suitable measures that cloud service users are able to satisfy themselves that the technical and organizational requirements pursuant to Section 9 BDSG are being met and that they are able to exercise the control rights (see TCDP No. 1.9) stipulated in the cloud contract.

Explanatory notes

Section 11 BDSG obligates cloud service users to satisfy themselves that the technical and organizational requirements are being met by the cloud service provider. Although this requirement can be fulfilled by simply checking the certification, there is a presumption that the cloud service user must nevertheless also have the right to carry out its own review.

Implementation guidance

The cloud service provider can provide and document a procedure through which the requests of the cloud service user are processed and the required cooperation of the cloud service provider is ensured. Such a procedure should enable the cloud service user to obtain information about the technical and organizational measures, to get answers to questions, and to carry out controls on location.

TCDP No. 10 – Returning and deleting data

Requirements

The cloud service provider must ensure through suitable measures that the data media entrusted to it are returned and the data stored by the cloud service provider is deleted after

the contract ends and is done so in accordance with the instructions of the cloud service user [ISO/IEC 27018 point A.9.3].

Implementation guidance

The cloud service provider can provide and document a procedure to regulate the return of data media and the deletion of data once the contract has ended. The cloud service provider can also satisfy the requirements by enabling cloud service users to delete the data themselves pursuant to a self-administration system. The implementation guidance provisions of ISO/IEC 27018 point A.9.3. are to be understood as non-compulsory guidelines.

TCDP No. 11 – Data privacy

Requirements

Any persons who work for the cloud service provider, its subcontractors, or any further subsubcontractor in the area of data processing of the cloud service user's data must, prior to beginning such data processing activity, be obligated pursuant to Section 5 BDSG or pursuant to other laws to maintain data privacy. The fact that such persons were put under obligation must be documented. An organizational procedure for obligating such persons must be established and documented.

Explanatory notes

The obligation to maintain data privacy does not necessarily have to be made a formal provision of the employment contract or a supplement to it. But the person must be instructed on it and put under the obligation prior to beginning the data processing work.

For persons working in the public sector who are already obligated by law to maintain data privacy, the obligating of them is not necessary. What is necessary, however, is that they be instructed on data privacy and on how long it is binding on them.

Implementation guidance

The obligation to maintain data privacy or the instructing on it are meant to raise the awareness of the persons involved for the issues of data protection and data security in relation to their work. An official copy of the obligation text together with the relevant excerpts from the applicable data protection act (e.g. reproduction of Sections 5, 43, 44 BDSG) should be handed out to them. The instructing must be repeated in reasonable intervals, for example in conjunction with training sessions.

The documentation of the obligating of the person must at least contain the information as to who, when, and with which content was obligated to maintain data privacy or was instructed

on data privacy. It is advisable to keep an official copy of the obligation document that was signed by the person.
The documentation of the procedure must stipulate who is responsible for obligating or instructing the persons; who, when, and in which way this is to be carried out; which persons have to be put under obligation or instructed and at which time; and what verification has to be kept about the obligating or the instructing and where and how long it has to be kept.

3. Technical and organizational measures

TCDP No. 21 – Security concept

Requirements

The cloud service provider must have a risk-appropriate security concept with respect to the risks specific to its service and its data processing facilities. The security concept must also stipulate the security measures that must be complied with by the cloud service user. It must be documented in writing and regularly reviewed and updated. Any security measures demanded of the cloud service user in the security concept must be communicated to the cloud service user in text form.

Explanatory notes

Technical and organizational measures must be risk-appropriate as understood by the statutory standards. The calculation and rating of risks and the appropriate security measures derived from such are generally the customer's responsibility in the case of outsourced data processing. According to the TCDP Concept of Categories of Protection Needs, the cloud service user must ascertain its own protection needs and must determine which category of protection needs it is in. This category of protection needs corresponds to the respective category of protection requirements of the cloud service provider. The cloud service user's security concept and the category of protection needs chosen by it are not reviewed within the framework of the TCDP.

The cloud service provider also has to have a security concept that deals with the risks specific to it and that defines the protection strategies appropriate to these. For example the computing centre in which the cloud service provider operates could be located in an earthquake endangered zone and therefore measures would have to be taken against tremors. Or the computing centre might be easily accessible via the roof of a neighbouring building and therefore precautions would have to be taken to prevent unauthorized physical access via the roof.

The only thing being reviewed here is whether a security concept exists and whether it is appropriate. The review of the appropriateness of the individual technical and organizational

security measures contained in the concept and the review of the implementation of them are the subject matter of the following numbers of the TCDP.

Implementation guidance

The security concept should cover the risks arising from the specific circumstances of the cloud service, its data processing facilities, and its physical premises and it should contain one or even several security measures for dealing with each risk.

The implementation guidance provisions of ISO/IEC 27018 point 5.1.1, ISO/IEC 27017 points 5.1.1 and CLD 6.3.1, and ISO/IEC 27002 point 5.1 are to be understood as non-compulsory guidelines.

TCDP No. 22 – Security area and physical access controls

Requirements

The controls set out in ISO/IEC 27002 point 11.1 must be understood as compulsory requirements.

Explanatory notes

Protection against damage caused by natural phenomena is addressed primarily within the framework of data loss prevention (restorability). Indirectly, however, it is also required for preventing physical access by unauthorized persons.

Implementation guidance

The implementation guidance provisions of ISO/IEC 27002 point 11.1. are to be understood as non-compulsory guidelines.

Implementation guidance to the protection categories

Protection category 1

The cloud service provider must ensure through risk-appropriate technical and organizational measures that its premises and facilities are secured against damage caused by natural phenomena and that unauthorized persons do not obtain physical access to its premises and data processing facilities.

The measures must be capable, in the normal case, of preventing the physical access of unauthorized persons resulting from the technical or organizational errors, including the operating errors, of the cloud service provider or its employees or from the negligent acts of third parties. A minimum amount of protection must be provided to make intentional intrusions more difficult to achieve.

Protection category 2

In addition: The measures must also be capable, in the normal case, of preventing damage caused by the negligent acts of authorized persons. Protection against intentional and unauthorized physical access must be provided in a way that adequately prevents expectable attempts of such. This particularly includes the adequate prevention of known attack scenarios and the use of measures through which unauthorized physical access is in normal cases (subsequently) identifiable.

Protection category 3

In addition: It must be ensured that unauthorized physical access caused by negligent and intentional acts is adequately prevented. This includes protection against attempts of physical accessing through deception or force. Every physical access and every attempt of such must be capable of identification.

TCDP No. 23 – Logical access to data processing facilities and access to data

Explanatory notes

The requirements in relation to physical access and access controls in Nos. 2 and 3 of the Annex to Section 9 sent. 1 BDSG are practically impossible to separate. In the ISO/IEC standards, for example, they are combined. This approach is also taken by the TCDP. In the case of cloud services, obligations are imposed on both the cloud service provider and the cloud service user with respect to the accessing of data. The TCDP only addresses the obligations of the cloud service provider.

Requirements

(1) The controls set out in ISO/IEC 27017 points CLD.9.5.1 and CLD.13.1.4 and in ISO/IEC 27002 points 9 and 13.1.1 must be understood as compulsory requirements.

(2) The requirements pursuant to (1) above also apply to backup copies, traffic data, and metadata in so far as they contain personal data.

Implementation guidance

The implementation guidance provisions of ISO/IEC 27018 points 9.2, 9.2.1, and 9.4.2, ISO/IEC 27017 points 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.4.1, 9.4.4, 13.1.3, CLD.9.5.1, and CLD.13.1.4, ISO/IEC 27002 points 6.1.5, 9, and 13.1.1 are to be understood as non-compulsory guidelines.

Implementation guidance to the protection categories

Protection category 1

The cloud service provider must ensure through risk-appropriate technical and organizational measures that unauthorized persons are unable to obtain physical access to data processing facilities and are unable to access personal data. The measures must be capable, in the normal case, of preventing physical access to data processing facilities by unauthorized persons and access to data resulting from the technical or organizational errors, including the operating errors, of the cloud service provider or its employees or from the negligent acts of the cloud service user or of third parties. A minimum amount of protection must be provided to make intentional intrusions more difficult to achieve.

Protection category 2

In addition: Protection against expectable and intentional unauthorized physical access [to data processing facilities] and access [to data] must be provided in a way that adequately prevents expectable attempts of such. This particularly includes the adequate prevention of known attack scenarios and measures through which unauthorized physical access [to data processing facilities] or access [to data] can normally be identified (subsequently).

Protection category 3

In addition: It must be ensured that the unauthorized physical accessing of data protection facilities and accessing of data is adequately being prevented. This regularly includes measures to actively identify attacks. Every unauthorized physical access [to data processing facilities] or access [to data] and any attempts of such must be capable of subsequent identification. What is generally required is the use of an identity access management system or an equivalent system for centrally documenting and managing the roles and rights of access to data. Access via the Internet requires strong authentication that uses at least two elements from the categories knowledge, possession, or inherency. These elements must be mutually independent in the sense that the breaching of one element does not compromise the integrity of the other/s. The authentication must also be designed in a way that ensures the confidentiality of the authenticating data.

TCDP No. 24 – Transferring and storing data

Requirements

The cloud service provider must use measures that are capable of ensuring that personal data is not being read, copied, altered, or removed in an unauthorized manner during the electronic transmission of it or during its transport or storage on data media and that through which it is possible to identify which group of recipients a transmission of personal data is intended for. In addition, a protocol of the transmission processes must be provided for [ISO/IEC 27018 points A.10.4, A.10.5, A.10.6, and A.10.9 and ISO/IEC 27002 points 8.3, 10, 12.4.1, 12.4.2, 12.4.3, and 13].

Explanatory notes

The aforementioned controls in ISO/IEC 27018 and ISO/IEC 27002 largely correspond, at least in terms of their content, to the statutory requirements of no. 4 of the Annex to Section 9 sent. 1 BDSG. The TCDP supplements the ISO/IEC standards by including measures that are not expressly addressed in the ISO/IEC standards. These concern measures that narrow the group of recipients from the outset and measures requiring protocols of transmissions to recipients that are not simultaneously users of the system.

Implementation guidance

The implementation guidance provisions of ISO/IEC 27018 points 10.1.1, A.10.6, and A.10.9, ISO/IEC 27017 points 13.1.3, and ISO/IEC 27002 points 8.3, 10, 12.4.1, 12.4.2, 12.4.3, and 13 are to be understood as non-compulsory guidelines.

Implementation guidance to the protection categories

Protection category 1

The cloud service provider must ensure through risk-appropriate technical and organizational measures that unauthorized persons are unable to read, copy, alter, or remove personal data during the transmission or storing of it.

The measures must be capable, in the normal case, of preventing these acts of unauthorized persons resulting from the technical or organizational errors, including the operating errors, of the cloud service provider or its employees or from the negligent acts of the cloud service user or of third parties. The measures must also be capable, in the normal case, of preventing the negligent transmission of data to unauthorized parties by the cloud service provider and its employees.

This also includes the transporting of data media that contain data of the cloud service user. A minimum amount of protection must be provided to make intentional intrusions more difficult to achieve. Which recipients a transfer of personal data is intended for must be documented. Automatic protocols must be made of data transfers, including those to the cloud service user or to subcontractors. The transport and the delivery of possession of data media must be documented. These measures must also cover the transferring of data within the cloud service provider's own networks and within its subcontractors' own networks and within the networks between them.

Protection category 2

In addition: Protection against the intentional and unauthorized reading, copying, altering, or removing [of data] must be provided in a way that adequately prevents expectable attempts of such. This particularly includes the adequate prevention of known attack scenarios and measures through which an unauthorized reading, copying, altering, or removing [of data] can normally be identified (subsequently). In the case of encrypted storage and transfers, technical and organizational measures must be in place to ensure that the cloud service provider has no access to the cipher keys that would enable it to read the personal data.

Protection category 3

In addition: It must be ensured that an unauthorized reading, copying, altering, or removing of data by the cloud service provider, its employees, or third parties is adequately prevented. This regularly includes measures to actively identify attacks and to ward off attacks. Every unauthorized reading, copying, altering, or removing of data and if possible every such attempt of such must be capable of being subsequently identified.

TCDP No. 25 – Transparency of the data processing

Requirements

(1) The control provisions in ISO/IEC 27002 point 12.4 must be understood as compulsory requirements. The principles of necessity, purpose limitation, and data minimization must be adhered to in the protocols.

(2) The cloud service provider must create a protocol concept that particularly documents the objects and the scope of protocols, storage policies, integrity protection and deletion of protocols, the use of protocol data, and the adherence to data protection goals in conjunction with protocols.

Explanatory notes

Because protocols often contain personal data, the handling of protocol data is itself governed by data protection law. To make this clear, TCDP No. 25 expressly includes the obligation to observe the principles of data protection law.

Implementation guidance

The implementation guidance provisions of ISO/IEC 27018 points 12.4.1 and 12.4.2, ISO/IEC 27017 points 12.4.1 and 12.4.4, and ISO/IEC 27002 points12.4 are to be understood as non-compulsory guidelines.

Implementation guidance to the protection categories

Protection category 1
The cloud service provider must ensure through risk-appropriate technical and organizational measures that it is possible to subsequently review and identify whether and by whom personal data was entered in, altered in, or deleted from data processing systems.

The measures must be capable of ensuring that the entering, altering, or deleting of data effected through the contractually conform use of the service by the cloud service user and through the administrative activities of the cloud service provider are transparent at all times.

The measures used for this, for example protocols of administrative activities and of the user's activities, must be designed in a way that preserves the transparency [i.e. traceability] of the entries, alterations, and deletions in normal cases and even in the event of technical and organizational errors, including operating errors, of the cloud service provider or its employees or in the event of negligent acts of the cloud service user or of third parties. A minimum amount of protection must be provided to make intentional manipulations of the traceability measures more difficult to achieve.

Protection category 2
In addition: Protection against expectable and intentional manipulations of protocol instances and against intentional accessing or manipulations of protocol files (logs) by unauthorized parties must be provided in a way that adequately prevents expectable attempts of manipulation. This particularly includes the adequate prevention of known attack scenarios and measures through which a manipulation can normally be identified (subsequently).

Protection category 3
In addition: It must be ensured that manipulations of protocol instances and files (logs) are being adequately prevented. This regularly includes measures to actively identify manipulations. Every manipulation and if possible every such attempt must be capable of being subsequently identified.

TCDP No. 26 – Instruction control

Requirements

The cloud service provider must ensure through risk-adequate measures that the processing of the cloud service user's data is only being done pursuant to the instructions of the cloud service user.

Explanatory notes

According to the law, a cloud service provider may only process data in accordance with the instructions of the cloud service user. The binding nature of the cloud service user's instructions must be agreed in the contract (see TCDP No. 1.11). The cloud service provider must also ensure that a processing of data is only carried out on the basis of such an agreement (see TCDP No. 2). And finally, the adherence to these instructions must be secured through technical and organizational measures. This is the object of TCDP No. 26. It is a widespread and permitted practice among cloud service users to issue their instructions in the form of software commands that are automatically executed by the cloud service provider.

Implementation guidance

There are no general implementation guidance provisions for TCDP No. 26. The implementation guidance provisions for the protection categories apply.

Implementation guidance to the protection categories

Protection category 1

The cloud service provider must ensure through risk-adequate technical and organizational measures that the processing of the cloud service user's data is only being done pursuant to the instructions of the cloud service user.

The measures must be capable, in the normal case, of preventing deviations from the instructions resulting from the technical or organizational errors, including the operating errors, of the cloud service provider or its employees or from the negligent acts of the cloud service user or of third parties. A minimum amount of protection must be provided to make intentional intrusions more difficult to achieve.

Protection category 2

In addition: The measures must adequately prevent expectable and intentional deviations from the instructions and must ensure that in the normal case intrusions can be identified (subsequently).

Protection category 3

In addition: It must be ensured that deviations from the cloud service user's instructions are being adequately prevented. This regularly includes making comprehensive protocols of administrator accessing and using measures that make interferences, including by the administrators, with the data to be processed and with the data processing activities contrary to the user's instructions considerably more difficult to achieve.

TCDP No. 27 – Separate processing

Requirements

The cloud service provider must ensure through suitable measures that data collected for different purposes can be processed separately.

Implementation guidance

There are no general implementation guidance provisions for TCDP No. 27. The implementation guidance provisions for the protection categories apply.

Implementation guidance to the protection categories

Protection category 1

The cloud service provider must ensure through risk-appropriate technical and organizational measures that the data of the cloud service user is being processed separately from the data bases of other cloud service users and from other data bases of the cloud service provider and that the cloud service user can separate the data processing according to different processing purposes. Examples of this include the isolation of the different tenants on the application side and the multitenancy ability of the software applications. The measures must be designed in such a way that in the normal case the data is being kept separate even in the event of technical and organizational errors, including operating errors, on the part of the cloud service provider or its employees or in the event of negligent acts of the cloud service user or of third parties. A minimum amount of protection must be provided to make intentional violations of the separation principle more difficult to achieve.

Protection category 2

In addition: Protection against expectable and intentional infringements must be provided in a way that adequately prevents them. In the area of data storage, this includes encryption with separate cipher keys and the use of separate operating environments for the different processing activities or the use of equivalent processes. In addition, measures must be use to

enable, in the normal case, the (subsequent) identification of intentional violations of the separation principle, for example through protocols of access instances.

Protection category 3

In addition: It must be ensured that adequate prevention of violations of data separation is being provided. In the area of data storage, this includes encryption with separate cipher keys and the use of separate operating environments for the different processing activities. There must also be a procedure for identifying abuses.

TCDP No. 28 – Cryptography

Requirements

Where the cloud service provider uses cryptographic processes, the controls set out in ISO/IEC 27002 point 10 must be understood as compulsory requirements.

Implementation guidance

The implementation guidance provisions of ISO/IEC 27018 point 10.1.1 and ISO/IEC 27002 point 10 are to understood as non-compulsory guidelines.

Implementation guidance to the protection categories

Protection category 1

The cloud service provider must ensure that it is keeping abreast of the technical developments in the area of cryptography and that the measures employed by it are up to current technical standards (suitability of the measures). In this respect, the appropriate implementation of the measures must be reviewed and documented using suitable tests.

Protection category 2

The cloud service provider must ensure that it is constantly keeping abreast of the technical developments in the area of cryptography and that the measures employed by it are up to current technical recommendations (best practices). In this respect, the appropriate implementation of the measures must be reviewed and documented using suitable tests.

Protection category 3

The cloud service provider must ensure that it is constantly keeping abreast of the technical developments in the area of cryptography and that the measures employed by it are up to current technical recommendations (best practices). In this respect, the appropriate implementation of the measures must be reviewed by independent expert bodies. The review and the results of it must be documented.

4. Restorability

TCDP No. 31 – Protection against accidental destruction or loss (restorability)

Explanatory notes

The requirements applicable to the restorability of data are not geared towards the three protection categories but are stated as three separate levels of restorability: “normal restorability”, “high restorability”, and “very high restorability”.

The restorability protection of the TCDP is geared towards the ability to restore data processed in the cloud service in the event of an accidental destruction or loss on the part of the cloud service provider. The restorability protection does not concern the availability of the service itself. This is typically regulated in a service level agreement (SLA) between the cloud service provider and the cloud service user.

Requirements

(1) The cloud service provider must have a concept for warranting the restorability of data and must provide the cloud service user with it upon the latter’s request.
(2) The cloud service provider must specify in the cloud contract the maximum time needed to restore data.

The cloud service provider must ensure through risk-adequate measures that the data can be restored within the time period specified in the cloud contract. The controls set out in ISO/IEC 27002 points 11.1.4, 11.2.1, 11.2.2, 11.2.4, 12.1, 12.2, 12.3, 12.6, and 12.7 must be understood as compulsory requirements.

Implementation guidance

The implementation guidance provisions of ISO/IEC 27018 point 12.3.1, ISO/IEC 27017 points 12.1.3 and 12.3.1, and ISO/IEC 27002 points 11.1.4, 11.2.1, 11.2.2, 11.2.4, 11.2.6, 12.1., 12.2, 12.3, 12.6, 12.7 and 17.2 are to be understood as non-compulsory guidelines.

Implementation guidance to the restorability levels

Normal restorability

Protection must be provided against expectable and probable events and it must be so reliable that in the ordinary course of events, these risks do not lead to permanent data loss.

High restorability

Protection must be provided against rare events and it must be so reliable that in the ordinary course of events, these risks do not lead to permanent data loss.

Very high restorability

Protection must be provided against exceptional albeit not theoretically impossible events and it must be so reliable that in the ordinary course of events, these risks do not lead to permanent data loss.

Natural phenomena (e.g. weather, state of the weather, storms, flood)s, breakdowns in the infrastructure (e.g. power, air conditioning), operational disruptions, operational errors, or negligent or intentional intrusions are all deemed to be “events”.

Explanatory notes

“Expectable and probable” means events that should not happen but, despite the fact that sufficient caution is exercised, experience shows that they cannot be ruled out completely and that they do happen “over and over again”, for example traffic accidents.

“Rare” means events that should not happen and according to experience “practically never” do happen when sufficient caution is exercised but that nevertheless do happen in some cases, for example a “100-year flood”.

“Exceptional albeit not theoretically impossible” means events that should not happen and according to experience do not happen but that nevertheless do happen in extremely seldom isolated cases, for example the so-called “black swan” events.

Endnotes

[1] On the working group “Legal Framework of Cloud Computing”, see [in German] http://www.digitale-technologien.de/DT/Navigation/DE/Foerderprogramme/Trusted_Cloud/Rechtliche_Fragen/rechtliche-fragen.html.

[2] Discussion paper “Solutions under Data Protection Law for Cloud Computing”, available [in German] at http://www.tcdp.de/index.php/start.

[3] Discussion paper “Modular Certification of Cloud Services “, available [in German] at http://www.tcdp.de/index.php/start.

[4] Discussion paper “Cornerstones of a Certification Procedure for Cloud Services”, available [in German] at www.tcdp.de.

[5] 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.

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

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

[8] ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

[9] For additional information [in German] on the pilot project, see http://www.tcdp.de/index.php/pilotprojekt.

[10] Working paper “Protection Categories in the Data Protection Certification” available [in German] at http://www.tcdp.de/index.php/start.

[11] Working paper “Protection Categories in the Data Protection Certification” available [in German] at http://www.tcdp.de/index.php/start.

[12] TCDP Concept of Categories of Protection Needs for the Data Protection Certification of Cloud Services 1.0, September 2016, available [in German] at http://www.tcdp.de/index.php/start.