European Cloud Service
Data Protection Certification

Determination Activities for the AUDITOR Criteria Catalogue

- Version 0.99f -

Status: 04/05/2022

Related AUDITOR publications:

- certification object
- criteria catalogue
- conformity assessment scheme
- concept of modularity
- concept of protection categories
- DIN SPEC 27557

Available online at: www.auditor-cert.de

Contribution to the research project "European Cloud Service Data Protection Certification (AUDITOR)," which, based on a resolution adopted by the German Parliament), is sponsored by the Federal Ministry for Economic Affairs and Energy (FKZ 01MT17003A).

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

Authors

Ali Sunyaev[a], Alexander Roßnagel[b], Sebastian Lins[a], Natalie Maier-Reinhardt[b], Johannes Müller[b], Heiner Teigeler[a]

[a] Research group: Critical Information Infrastructures (cii) of the Institute of Applied Informatics and Formal Descriptive Methods (AIFB) at the Karlsruhe Institute of Technology

[b] Project group: Constitutionally Compatible Technology Design (provet) at the Research Centre for Information Technology Design (ITeG) at the University of Kassel

Table of contents

List of abbreviations and acronyms

Alt.	Alternative
Art.	Article
BDSG	Federal Data Protection Act (applicable as of 25.05.18)
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
ECJ	The Court of Justice of the European Union
DPO	Data Protection Officer
E.g.	For example
EEA	European Economic Area
EU	European Union
GDPR	EU General Data Protection Regulation (applicable as of 25.05.18)
GTC	General Terms and Conditions
Lit.	Litera (letter)
No.	Number
Para.	Paragraph
SDM	Standard Data Protection Model
Sec.	Section
Subpara.	Subparagraph
TCDP	Trusted Cloud Data Protection Profile
The Charter	Charter of Fundamental Rights of the European Union
TOM	Technical and organisational measures

Note on the gender-neutral wording:

All references to persons in the AUDITOR Criteria Catalogue shall be considered to be gender-neutral. Therefore, for the purpose of better readability, no gender-specific wording is used, while the male grammatical form shall apply to all genders equally (e.g., any use of the title “data protection officer” in combination with male pronouns is a reference to the functional description as gender-neutral and without specifically referring to a person of the male gender).

A. Guide for assessing the AUDITOR Criteria Catalogue

1. Introduction

The AUDITOR certification provides evidence of the compliance of cloud providers' data processing operations with the requirements of the EU General Data Protection Regulation (GDPR). Pursuant to Art. 43 (1) sentence 1 GDPR, certification bodies may issue certifications alongside data protection supervisory authorities. However, a certification body may only commence its activities if it has been accredited by the German Accreditation Body (Deutsche Akkreditierungsstelle GmbH; DAkkS) in cooperation with the responsible data protection supervisory authority. The prerequisite for accreditation is compliance with the requirements pursuant to Art. 43 (2) of the GDPR and the supplementary requirements of the German Data Protection Conference (“Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder”; DSK) for accreditation pursuant to Art. 43 (3) of the GDPR in conjunction with ISO/IEC 17065.

Decisive for accreditation is a conformity assessment scheme, which must be developed for each certification individually. The AUDITOR conformity assessment scheme describes the principles to be fulfilled by the certification body and essentially includes requirements for the certification body and the certification process. The AUDITOR Criteria Catalogue, on the other hand, is a testing standard for the data protection certification of cloud services in accordance with the requirements of the GDPR. It contains "criteria", "explanations", “implementation guidance” and “proof”. The *"criteria"* describe the normative requirements to be fulfilled in order to receive a certificate on the basis of the AUDITOR Criteria Catalogue. The *"explanations"* are intended to make the understanding of the criteria and their derivation from the law easier. For each criterion, *“implementation guidance”* serve as guidance using typical examples for understanding and implementing the criteria; however, they are not binding. Moreover, for each criterion there is a *“proof”* section included, which provides the answer to the question of how it can be proven that the criteria are fulfilled in the specific certification mechanism. Similar to the implementation guidance, proof serves as guidance and provides informative help that is intended to support cloud providers, certification bodies, auditors, and other interested parties in assessing compliance with the criteria. There is no obligation to demonstrate compliance with the requirements in accordance with this document.

This document provides guidance on how to conduct determination activities to assess whether the AUDITOR criteria are met. Therefore, the document is structured according to the outline of the AUDITOR Criteria Catalogue. It represents a central extension of the AUDITOR conformity assessment scheme.

2. Use of this guide

The certification criteria represent the data protection requirements that data processing operations need to fulfill and can refer to different objects of determination, as can be seen in Table 1. For example, in Chapter 1 of the criteria catalogue, the legally binding agreement on commissioned processing forms the object of determination, while in Chapter 2, software architecture, infrastructure and processes will regularly play a role in ensuring data security according to No. 2. Figure 1 schematically illustrates the classification of objects of determination.

Object of determination	Description
Legally binding agreement	In the case of legally binding agreements as the object of determination, the characteristics and contents of contracts or agreements with cloud users or subcontracted processors are assessed.
Process	A process or a corresponding and realistic process documentation can be checked to confirm conformity with the certification criteria.
Provider characteristics	An examination of provider characteristics includes the assessment of characteristics and features of the cloud provider, for example, the underlying organisational structure.
Service characteristics	Service characteristics include, in particular, cloud service features and functions that are directly visible to the cloud user and must be verified.
Infrastructure components	An assessment can include infrastructure components, which are physical objects such as hardware components or the data centre infrastructure.
Software architecture	The testing of software architecture and its components includes virtual objects, for example, source code, as well as the composition and interactions of the individual components of data processing operations.
Development environment	Testing of the development environment includes development methods used, secure test and development environment separate from the production system, and acceptance tests.
Personnel	The examination of cloud provider's employees may be necessary, for example, to ensure their professional or personal suitability.
(data protection) management system	The audit of the (data protection) management system is necessary to identify whether the cloud provider has implemented a system for managing the relevant aspects of its activities, products and services that is in line with the organisation's policy and the certification criteria.

Table 1. Overview of possible objects of determination within a data processing operation.

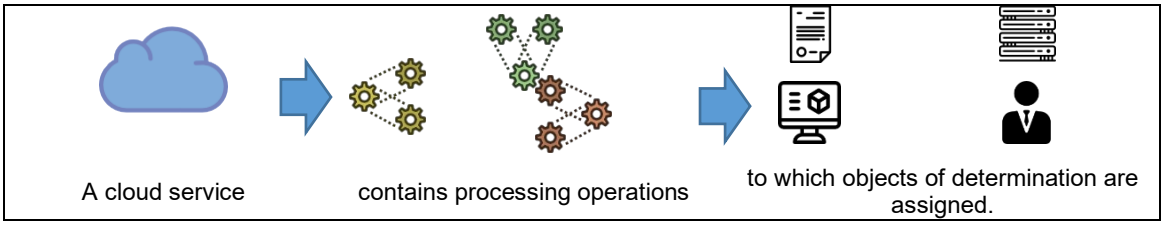

Figure 1. Schematic representation for the classification of objects of investigation.

For each criterion, "*determination methods*" and a description of the "*determination activities*" are given. As part of the determination activities, one or more determination methods (e.g., document review or auditing) are performed to obtain complete information on the compliance of the data processing operations or their samples with the criteria specified in the AUDITOR Criteria Catalogue. The following paragraphs summarise possible determination methods according to the AUDITOR conformity assessment scheme, which can be applied in the context of a certification:

1. **Document review** (in the sense of ISO/IEC 17020**)**. With the document review, the evaluator verifies compliance with the certification criteria based on the information in the cloud provider's documentation. A cloud provider submits corresponding documents, (technical) logs, certificates or other documentation. A legal analysis takes place (e.g., of the legally binding agreements) to ensure that the applicable legal criteria are met. In addition, certificates of persons (in the sense of ISO/IEC 17024) for proof of competence for the personnel or a natural person (e.g., the data protection officer) and to ensure an appropriate level of data protection can be assessed within the scope of a document review. A document review must always be supplemented with appropriate determination methods to ensure that the documented instructions, procedures, rules, etc. are also continuously implemented by the cloud provider.

2. **Inspection** (in the sense of ISO/IEC 17020). An inspection examines the conformity of a product or process with specific requirements (in this case the GDPR and the certification criteria). Inspection parameters include questions about the quantity, quality, safety, suitability, and continued compliance with the safety of equipment or systems in operation. Regarding the AUDITOR certification, compliance with appropriate technical and organisational measures pursuant to Art. 32 (1) a) to d) of the GDPR is examined by means of a (legal) inspection. The inspection can concern all phases within the scope of the life cycle of the objects of determination, including the development phase. During the inspection, data processing operations can be carried out in the context of service use, for example, to be able to assess the functioning and the results of the operations. An evaluator compares the expected results according to the available documentation with the actual output resulting from a service use. Thus, the evaluator has no insight into the internal processing steps of the processing operations

('black box test'). In addition, a process or a series of processes can also be initiated and the actual execution monitored ('monitoring') or logs of the process execution checked ('white box test').

3. **Testing** (as defined in ISO/IEC 17025:2017). A test involves means and measurements to examine the data processing operation or the certification object and to determine their compliance with the certification criteria. For example, an asset test may be conducted by examining an asset (e.g., hardware or software code and associated documentation, if applicable). The test may be conducted in the company of, or under the instruction of an employee of the cloud provider, or independently by the evaluator. The cloud provider must be informed in advance about the test and provides the evaluator with, for example, necessary access (e.g., test accounts) or (technical) logs about the execution of the process for performing the test. If necessary, the evaluator selects suitable test data. This includes randomly generated values which allow a realistic and functionally compliant testing of the operation. An evaluator may use appropriate testing products and services (provided externally where appropriate) to test and monitor the process (see ISO/IEC 17025:2017 subs 6.6). The testing products and services used shall be documented in the determination report. In the case of invasive test procedures or procedures that could lead to an impairment of data processing operations of the cloud service, coordination with the cloud provider is necessary. The cloud provider is obliged to support the evaluator in the implementation. Regarding the AUDITOR certification, the compliance with suitable technical and organisational measures pursuant to Art. 32 (1) a) to d) of the GDPR is checked by means of a (legal) test. For example, security tests can be used to determine the correct and strong encryption of data. When conducting security tests, please refer to ISO/IEC 15408:2009 and ISO/IEC 18045:2008-018.

4. **Audit** (as defined in ISO/IEC 17021-1:2015). An audit is performed for the purpose of certifying the cloud provider's (data protection) management system (see ISO/IEC 17021-1:2015 subs 3.4) to identify that the cloud provider uses a system for managing the relevant aspects of its activities, products and services that is in accordance with the organisation's policy and the certification criteria. Audits may be conducted on-site, remotely or a combination of both (see ISO 19011:2018-10 subs 5.5.3). The use of these methods should be appropriately balanced based on, among other things, consideration of the risks and opportunities involved. In particular, interviews, observations and exams may be conducted as part of the audit to determine information about knowledge and skills, as well as whether processes and the management system are practised by the cloud provider. Interviews with employees of the cloud provider or other persons involved in the provision of the data processing operations can be used to determine the facts of individual aspects and to check the correctness of the documentation (see ISO/IEC 17021-1:2015 subs. B.4). Interviews should be used in particular to check aspects identified as critical by the evaluator. Interviews can be conducted in writing or in person. They shall be conducted as oral interviews regarding central aspects. If an on-site interview would be disproportionate, it can be conducted in the form of video conferences. Observing a person performing a task can provide direct evidence of competence through the application of knowledge and skills thus demonstrated to achieve a desired outcome (see ISO/IEC 17021-1:2015 subs B.5). Written, oral and practical examinations can provide good and well-documented evidence of existing knowledge and, depending on the methodology used, skills (see ISO/IEC 17021-1:2015 subs B.6). An on-site audit includes an inspection of the procedures and technical equipment at the premises of the cloud provider. Regarding the AUDITOR certification, (legal) audits are to be carried out to verify the correct establishment, maintenance, and upkeep of a data protection management system (within the meaning of Art. 24 and 25, 32, 33, 34 as well as 37 to 39 GDPR). The establishment of a data protection management system should ensure the constant level of data protection of the certified cloud service. For further literature on performing audits, please refer to ISO/IEC 17021-1:2015 subs. 9.4 and ISO 19011:2018-10. For performing remote audits, please refer to IAF MD 4:2018.

5. **Development and design review** (in the sense of ISO/IEC 17020). A development review includes the review of development methods and procedures and, if required, a review of the test systems and environments used in the development of hardware and software to deliver the data processing operations. The design review may include review of the selected architecture, database diagrams, data flow diagrams, design decisions, but also the configuration of the cloud service to provide the data processing operations. A development and design review should also include a legal analysis to ensure that the applicable legal criteria are met. A legal design and development review may be required as part of the compliance review under Art. 25 GDPR or as part of the review of the data protection impact assessment.

   In the following, suitable determination methods and activities are discussed for each criterion. The relevant international standards on the determination methods must be taken into account when performing determination activities. The relevant international standards are ISO/IEC 17025 for testing, ISO/IEC 17020 for inspection, ISO/IEC 17021 for audits of management systems and ISO/IEC 17024 for certification of persons. An evaluator checks the suitability and application of the respective method depending on the certification object and the concrete object of determination. An evaluator must ensure that not only sufficient documentation is available as evidence, but also that the documented measures are implemented and practised (i.e., 'lived'). Especially in the case of determination activities within the AUDITOR data protection certification, a continuous legal analysis should be carried out. For example, in a document review, evaluators shall not only the review agreements, but also the concrete implementation of the cloud provider as a processor should be reviewed by means of suitable additional determination methods to ensure that the applicable legal criteria are fulfilled. If necessary, determination methods can be combined in order to collect (additional) well-founded information about the object of determination. The determination activities can be carried out on a sample basis according to the guidelines of the conformity assessment scheme.

B. Criteria and determination activities of Commissioned Data Processing

Chapter I: Legally binding Commissioned Data Processing Agreement

Explanation

The cloud provider must ensure that the services are provided for the cloud user on the basis of a legally binding agreement[1] fulfilling the legal requirements for Commissioned Data Processing under the General Data Protection Regulation. The legal requirements for this agreement are specified by the following criteria under numbers 1.1 to 1.8.

No. 1 – Effective and clear agreement between cloud provider and cloud user (Art. 28 (3) GDPR)

No. 1.1 – Service on the basis of a legally binding agreement and form of the agreement (Art. 28 (3) subpara. 1 sent. 1 and (9) GDPR)

Criterion

(1) The cloud provider must ensure by means of TOM that the cloud service is provided only after a legally binding Commissioned Data Processing Agreement is concluded with the cloud user.

(2) The legally binding agreement must be documented in writing or in an electronic form.[2]

(3) This agreement must meet the criteria of this chapter (no. 1.2 to 1.8) meanwhile the specifications of these criteria may also be defined in other documents if these have been included as part of the legally binding Commissioned Data Processing Agreement.

Explanation

The legally binding Commissioned Data Processing Agreement is essential because it explicitly clarifies the role of the cloud provider as a processor within the meaning of Art. 4 no. 8 GDPR compared to the role of the cloud user as a controller. This agreement is often based on another service agreement; it must be differentiated between the two agreements.

Implementation guidance

The cloud provider takes TOMs to ensure that the agreement is concluded automatically before the service is actually used. For this purpose, an accordant agreement may be displayed to the potential cloud user during the (electronic) registration, which must then be confirmed by the user before he uses the service.

In case of standardised bulk transactions, standard contractual clauses (general terms and conditions, or GTC) are used in the normal case, even among companies, which must be effective within the meaning of the respective GTC law.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 8.2.

Determination methods

- Document review, particularly legal analysis
- Inspection

Determination activities

The evaluator checks the conclusion of standardised agreements against a sample of agreements from the database (or another location where agreements are stored). The elevator should also randomly check an agreement's conclusion date against the timestamp of the initial creation of the user record. If no standardised agreements have been concluded, an evaluator checks all or a representative sample of legally binding agreements that a cloud provider has concluded with the cloud users as part of the document review.

[1] Art. 28 (3) subpara. 1 sent. 1 GDPR regulates the processing on the basis of a processing contract. Alternatively to the contract, another legal instrument in accordance with Union law or the law of the Member States as defined by Art. 28 (3) subpara. 1 sent. 1 GDPR may apply as the legal basis for the processing.

[2] For the electronic form, the text form as defined by Sec. 126b BGB (German Civil Code) suffices.

A representative sample should be chosen at least broad enough to ensure that a comparative review of a selection of agreements is highly likely to exclude the possibility that any other agreement is materially different. The sample size is therefore also dependent on the total number of agreements concluded. Evaluators should aim for a sample size of usually 3%. The individual agreements can be combined into groups, whereby a sufficient number of agreements from each group of agreements must be examined. Agreements can be grouped according to, among others, the subject matter, the duration, the nature, and the purpose of the processing.

Based on suitable documentation (e.g., process documentation, function documentation, or log files), the evaluator must check whether the cloud provider has taken technical or organisational precautions to ensure automatic agreement closure before the actual service use (e.g., concerning an agreement or registration process with potential cloud users). This function documentation must make it clear to an evaluator that a potential cloud user can only perform a data processing operation if a legally binding agreement is concluded in accordance with the specifications of the criteria catalogue.

In addition, an evaluator should perform an inspection in the form of a test execution of a corresponding agreement or registration process to ensure that the concepts specified in the documentation have also been implemented in the cloud service. As part of the test execution, an evaluator should also check whether the conclusion of an agreement can be circumvented by intent or misconduct.

No. 1.2 – Subject-matter and duration of the processing (Art. 28 (3) subpara. 1 sent. 1 GDPR)

Criterion

(1) The subject-matter and the duration of the processing must be defined in as much specificity as possible in the legally binding Commissioned Data Processing Agreement.

(2) The agreement must specify the duration of the processing by a start and an end point or refer to an indefinite period of use.

Implementation guidance

By means of the restriction of the subject-matter of the agreement, it should be clear to both parties which processing operations or categories are carried out by the cloud provider for the cloud user. In particular, the agreement should detail in a transparent manner what opportunities the cloud provider has for influencing the choice of processing means that are used to implement the processing operations involving personal data. Regulations on the processing subject-matter should also reflect the defined areas of responsibility between cloud users and cloud providers.

Reference is made to the implementation guidance for the transparent system description in BSI C5, UP-01 as well as the distribution of responsibility in OIS-03.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 8.2.

Determination methods

- Document review, particularly legal analysis
- Inspection

Determination

Through a document review (in particular, review of contract samples, templates, or instances provided by the cloud provider) and inspection in the form of service use (in particular, inspection of whether relevant content is displayed during service use), the evaluator verifies that the subject-matter and duration of the contract are specified and communicated to the cloud user in an appropriate manner.

No. 1.3 – Nature, scope and purposes of data processing (Art. 28 (3) subpara. 1 sent. 1 GDPR)

Criterion

The legally binding agreement on Commissioned Data Processing must determine the scope, nature and purpose of the intended data processing in the order, the nature of data processed in accordance with the concept of protection categories and the categories of data subjects.

Implementation guidance

Although these individual details do not have to cover every specific individual case, they should be precise enough to allow comprehension from the cloud user's point of view of the data processing operations that are permissible in the course of the Commissioned Data Processing.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 8.2 and ISO/IEC 27018 no. A10.11.

Determination methods

- Document review, particularly legal analysis
- Inspection

Determination activities

Through a document review (in particular, review of contract documents, templates, or instances provided by the cloud provider) and an inspection in the form of service use (in particular, inspection of whether relevant content is displayed during service use), the evaluator checks whether the scope, nature, and purpose of the data processing, the nature of data processed in accordance with the concept of protection categories, and the categories of data subjects are specified and communicated to the cloud user in an appropriate manner.

No. 1.4 – Determination of authority of the cloud user (Art. 28 (3) subpara. 1 sent. 2. lit. a) and h), subpara. 2 GDPR)

Criterion

(1) The legally binding Commissioned Data Processing Agreement must provide that the personal data will only be processed upon documented instruction by the controller – also with regard to transfers of personal data to a third country or an international organisation, unless the cloud provider is obligated to do so by Union or Member State law that applies to it.

(2) In the event that the cloud provider is obligated by Union or Member State law to process data, the legally binding Commissioned Data Processing Agreement must provide for the obligation of the cloud provider to inform the cloud user of the legal requirements prior to the processing, unless such law prohibits the information on important grounds of public interest.

(3) In the event that the Commissioned Data Processing intends transfers of personal data to third countries or international organisations bound by instructions, the legally binding Commissioned Data Processing Agreement must specify the instruments to be used for the transfers in accordance with Art. 45 GDPR or Art. 46 (2) and (3) GDPR and, if necessary, which supplementary measures have to be taken to ensure an adequate level of protection.

(4) If no individual legally binding agreement is entered into within the framework of standardised bulk transactions, the cloud provider must name in its service description, in as much detail as possible, the services it can technically perform in a manner that is comprehensible from a cloud user's perspective so as to enable a selection in accordance with Art. 28 (1) GDPR.

(5) In the legally binding Commissioned Data Processing Agreement, the cloud provider must undertake to inform the cloud user if, in its opinion, an instruction of the cloud user violates data protection provisions.

Explanation

The dependence on instructions is referred to at multiple junctures in the General Data Protection Regulation (Art. 28 (3) subpara. 1 sent. 1, lit. a); Art. 28 (3) subpara. 1 sent. 3 GDPR and indirectly in Art. 28 (10) and Art. 29, Art. 32 (4) GDPR).

If the cloud provider transgresses the determinations made by the cloud user in accordance with its instructions, there is a violation in accordance with Art. 28 (10) and Art. 29 GDPR, and the cloud provider must expect consequences under liability regulations.

According to Art. 28 (3) subpara. 1 sent. 2, lit. a) GDPR, compliance with issued instructions cannot release the cloud provider from compliance with the law to the effect that the cloud provider may execute processing that is not covered by instructions if it is obligated to do so under Union or Member State law. This regulation is intended to prevent the cloud provider from conflicts of interests.

Implementation guidance

The legally binding Commissioned Data Processing agreement should make clear who has the authority to issue instructions and who is entrusted with receiving the instructions on the part of the cloud provider. The departmental and functional levels authorised to issue instructions and their means of authentication can be specified in the legally binding Commissioned Data Processing Agreement.

The technically feasible services and the cloud user's authorities to issue instruction should be listed in the legally binding Commissioned Data Processing Agreement of the cloud provider. The legally binding agreement should set out the options available to the cloud user to exercise its authority for issuing instructions. In particular, these can also be automated procedures (e.g., API requests or software commands). On the basis of the cloud provider's service description (unilaterally pre-defined in bulk transactions), the potential cloud users should receive information on their selection pursuant to Art. 28 (1) GDPR. Where this is the case, the cloud user is to instruct the cloud provider to perform the described, standardised service by selecting the cloud service.

The legally binding Commissioned Data Processing Agreement should indicate whether instruction bound data transfers to third countries or international organisations should be carried out as part of the Commissioned Data Processing and how an appropriate level of protection should be guaranteed there. Appropriate safeguards for a data transfer are e.g., standard data protection clauses of the Commission according to Art. 46 (2) lit. b) GDPR or approved certification mechanisms according to Art. 46 (2) lit. f) in conjunction with Art. 42 GDPR. In addition, supplementary measures should be specified, if no adequate level of protection can be achieved with the instruments according to Art. 46 (2) and (3) GDPR alone (see also no. 11.1).

Reference is made to the implementation guidance for the transparent system description in BSI C5, UP-01.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A2.1.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 8.5.1 and 8.5.2.

Determination methods

- Document review, particularly legal analysis
- Inspection

Determination

Through a document review (in particular, review of contract documents, templates, or instances provided by the cloud provider) and inspection in the form of service use (in particular, inspection of whether content is displayed during service use), the evaluator checks whether a service description explains the services that can be technically executed by the cloud user and specifies who is authorised to issue instructions; and who on the part of the cloud provider is entrusted with receiving the instructions, and how these specifications are communicated to the cloud user in a suitable manner. The evaluator also checks whether the cloud provider discloses information on processing that is not bound by instructions based on legal obligations under Union or Member State law and on the establishment of appropriate safeguards for data transfers to third countries or international organisations in legally binding agreements and contractually undertakes to inform the cloud user if it believes that an instruction from the cloud user violates data protection law.

In the context of a document review (in particular, review of sample contracts, templates, instances, or concluded contracts provided by the cloud provider), the evaluator also examines which instruments according to Art. 45 GDPR or Art. 46 (2) and (3) GDPR are used for the transfer of personal data to third countries or international organisations and, if applicable, which additional contractual, organisational and/or technical measures are contractually stipulated if the aforementioned instruments alone are not sufficient to establish an adequate level of protection.

No. 1.5 – Place of data processing (indirectly in Art. 28 (3) subpara. 1 sent. 2 lit. a) GDPR)

Criterion

(1) In the legally binding Commissioned Data Processing Agreement, it must be determined whether the cloud provider processes the data of the cloud user within the EU/EEA or in a third country.

(2) If the data processing is carried out in a third country, this must be specifically stated in the legally binding agreement.

(3) The legally binding agreement must provide that the cloud provider notifies the cloud user without undue delay in the event that the place of processing changes during its period of validity.

Explanation

The specific country in which the personal data are to be processed is to be specified only if the data processing takes place in a third country; whereas not if the data processing is to take place in the EU or the EEA.

Implementation guidance

Reference is made to the implementation guidance in ISO/IEC 27018 no. A11.1 and ISO/IEC 27701 no. 8.5.

Exclusive data processing in the EU or the EEA does not always prevent personal data from being automatically withdrawn from access by public authorities of third countries. For example, the Cloud Act can also require cloud

providers based in the EU, which are affiliated with a US parent company and process personal data exclusively in the EU or in the EEA, to disclose this personal data stored in the EU or in the EEA to US authorities.

Similar regulations may also apply in other national laws of third countries. Choosing cloud providers is not prohibited per se, but cloud users and cloud providers must find solutions to effectively protect personal data from access by the public authorities of the third country concerned. One possibility is, e.g., hiring a trustee who is subject exclusively to European law and who has exclusive access to the outsourced data of the cloud user. As a result of the trust agreement, the personal data are neither owned nor under the control of the cloud provider and could consequently not be released to US authorities. For some cloud services, encryption can also be a solution. See the use cases in no. 11.1 and the other explanations there.

Determination methods

- Document review, particularly legal analysis
- Inspection

Determination activities

Through a document review (in particular, review of contract documents, templates or instances provided by the cloud provider) and inspection in the form of service use (in particular, inspection of whether content is displayed during service use), the evaluator checks whether the location of the data processing (within the EU/EEA or the specific third country) and the obligation to report changes in the location are specified and communicated to the cloud user in an appropriate manner.

No. 1.6 – Confidentiality obligation (Art. 28 (3) subpara. 1 sent. 2 lit. b) and h) GDPR)

Criterion

> The cloud provider undertakes by way of the legally binding Commissioned Data Processing Agreement to impose confidentiality obligations on the persons authorised to process personal data before they begin with the data processing activity, which shall also continue to apply even beyond the end of their employment, unless they are already subject to an appropriate, comparable statutory confidentiality obligation.

Explanation

The confidentiality obligation and secrecy instruction promote the protection goal of confidentiality (SDM C1.4).

The fact that the confidentiality obligation of the persons authorised to process personal data continues to apply beyond the end of their employment does not explicitly follow from the wording of Art. 28 (3) lit. b) GDPR. According to the meaning and purpose of the legal norm, however, this confidentiality obligation must continue to apply beyond the end of the employment, as otherwise no adequate protection of personal data can be guaranteed.

Implementation guidance

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.10.2.4.

Determination methods

- Document review, particularly legal analysis
- Inspection

Determination activities

An evaluator checks through a document review (in particular, by reviewing sample contracts, templates or instances provided by the cloud provider) that the cloud provider has made a legally binding commitment to oblige the persons authorised to process personal data to maintain confidentiality before commencing the data processing activity unless they are already subject to an appropriate comparable legal duty of confidentiality. Through an inspection in the form of a test use of the service, an evaluator can check whether these contents are specified and displayed to the cloud user in the legally binding agreement.

No. 1.7 – Technical and organisational measures, subcontracting and assistance (Art. 28 (3) subpara. 1 sent. 2 lit. c) to f) in conjunction with Ch. III and Art. 32 to 36 GDPR)

Criterion

(4) The protection category and the TOMs to be taken must be determined in the legally binding Commissioned Data Processing Agreement.

(5) The legally binding Commissioned Data Processing Agreement must include the statement of whether the cloud provider or cloud user carries out pseudonymisation, anonymisation or encryption (no. 2.7, no. 2.8 and no. 2.9) of the personal data, and whether this is also applicable to the staff of the cloud provider.

(6) In the legally binding Commissioned Data Processing Agreement, the cloud provider must determine at what level and how quickly (within what time frame) it can restore the cloud user's data and the cloud service after a physical or technical incident and guarantee the cloud user access to the cloud service and the data (No. 2.11).

(7) In the legally binding Commissioned Data Processing Agreement, it must be determined how the cloud provider complies with the requirements in accordance with Art. 28 (2) and (4) GDPR for the use of the services of other processors.

(8) The procedures and TOMs, which are to assist the cloud user in the fulfilment of data subjects' rights in accordance with no. 6, in carrying out a data protection impact assessment in accordance with no. 7, and in fulfilling the reporting obligation in the event of data protection breaches in accordance with no. 8.2, must be defined in the legally binding Commissioned Data Processing Agreement.

Implementation guidance

Information on implementing the criteria under no. 2 can be aligned with protection goals, while the specific measures for achieving the objectives can be left to the cloud provider. It is important for the cloud user to know the level of protection the cloud service offers.

The requirements of Art. 28 (3) subpara. 1 sent. 2 lit. d) GDPR should be specified in the legally binding Commissioned Data Processing Agreement so that compliance can be easily verified by the cloud user.

The cloud provider can specify a restorability period in the legally binding agreement and refer to the respective restorability class of the certification.

Since the cloud user has a right to object to changes in subcontracted processing (no. 10.3), the legally binding Commissioned Data Processing Agreement should address the prerequisites and consequences of an objection, such as whether the cloud user may terminate the agreement upon objection.

The legally binding Commissioned Data Processing Agreement should specify the cloud provider's support obligations, taking into account the design of the specific cloud service and the TOMs that are reasonable and appropriate for the cloud provider. This is to avoid uncertainties with regard to rights and obligations arising from the agreement.

Reference is made to the implementation guidance in ISO/IEC27018 no. A1.1 and A10.11 and ISO/IEC 27701 no. 6.13.1.5, 8.2.1, 8.2.5 and 8.3.1.

Determination methods

- Document review, particularly legal analysis
- Inspection

Determination activities

Through a document review (in particular, review of contract documents, templates or instances provided by the cloud provider) and an inspection in the form of service use (in particular, inspection of whether content is displayed during service use), an evaluator checks whether the procedures, processes and TOM to support the cloud user in fulfilling its obligations according to Art. 33-36 GDPR are defined and communicated to the cloud user in an appropriate manner. For this purpose, the corresponding documentation of the procedures and processes, such as those for reporting data protection violations to cloud users, can be examined.

In addition, the evaluator must check whether the cloud provider has specified and sufficiently described the TOMs used to ensure data security in accordance with Art. 32 GDPR in the agreement. Sufficient means that all TOM are described, and a level of detail is reached which, on the one hand, does not disclose any sensitive or security-critical information but, on the other hand, enables a cloud user to obtain sufficient information to assess the risk situation and the adequacy of the TOM. In this way, the specification of the TOM can be aligned with the protection goals. In order to assess compliance with the conditions of Art. 28 (2) and (4) GDPR, the evaluator checks the contract templates or instances provided by the cloud provider for the commissioning of subcontractors for completeness pursuant to Article 28 (3) GDPR and admissibility as part of a document review. See also the determination activities for criteria No. 10.1. to 10.5.

No. 1.8 – Return of data media and erasure of data (Art. 28 (3) subpara. 1 sent. 2 lit. g) and h) GDPR)

Criterion

The obligations of the cloud provider to return data media and return data or irreversibly delete data after the end of the data processing must be determined in a legally binding Commissioned Data Processing Agreement.

Explanation

If the cloud provider is obligated to store or keep data due to legal obligations even after the end of the Commissioned Data Processing, these data are not to be deleted.

Implementation guidance

Compliance with the requirements of returning data media and erasing data can also be demonstrated by reference to the corresponding principles of the cloud provider. The cloud user should be able to choose between the modalities of execution.

Determination methods

- Document review, particularly legal analysis
- Inspection

Determination activities

Through a document review (in particular, review of sample contracts, templates or instances provided by the cloud provider) and inspection in the form of service use (in particular, inspection of whether content is displayed during service use), an evaluator checks whether the cloud provider's obligations of returning data media and returning data to the cloud user and to erase data after the Commissioned Data Processing has ended are communicated to the cloud user in a suitable manner.

Chapter II: Rights and obligations of the cloud provider

No. 2 – Ensuring data security by appropriate state-of-the-art TOMs

No. 2.1 – Data security concept (Art. 24, 25, 28, 32, 35 in conjunction with Art. 5 (1) lit. f) and (2) GDPR)

Criterion

(1) The cloud provider must conduct a risk analysis with regard to data security and it must have a data security concept, which corresponds to its protection category and is appropriate for the specific risks of its data processing operations in particular, which can result from destruction, loss, alteration, unauthorised disclosure of and unauthorised access to personal data.

(2) The cloud provider must have a description of all data categories that it processes as a processor.

(3) In addition to the data security concept, the information required in no. 2 may also be made in other documents provided that this has been agreed upon bindingly in the Commissioned Data Processing between the cloud provider and cloud user. The requirements for the data security concept also apply to these other documents.

(4) In the data security concept, the cloud provider must specify which data security measures it has taken to eliminate or mitigate existing risks. The cloud provider must also describe the considerations it has made in order to arrive at these measures.

(5) The data security concept must be documented in writing or in electronic form.

(6) The data security concept must be reviewed at regular intervals to ensure that it is up to date and appropriate and be updated if necessary.

(7) The data security concept must describe which of the data processing operations are within the cloud provider's responsibility and which of the data processing operations are within the responsibility of the involved sub-processors.

(8) The data security concept must describe which data processing operations are within the cloud provider's responsibility and which are within the cloud user's responsibility.

(9) If the data security concept demands security measures from the cloud user, the cloud user must be informed of this in writing or in electronic form.

Explanation

The cloud provider must define risk-appropriate TOMs in order to prevent risks of violations of rights and freedoms of natural persons. In particular, it must exclude or minimise risks of accidental and unlawful destruction, loss, alteration, unauthorised disclosure of and access to personal data. When setting the specific measures, it will consider not only the methods of the processing and the likelihood and severity of damage, but also the state of the art and the costs of implementation of the measures. The considerations having been made in this regard must be reflected in the data security concept. The cloud user sets the category of protection requirements for its offered service. The cloud user selects a cloud service that offers a category of protection requirements suitable for its protection needs category.

Implementation guidance

The data security concept is to cover the risks arising from specific circumstances of the cloud service, its data processing operations, and its premises, and is to include various guidelines and security measures and specify resources, responsibilities, and prioritisations for handling information security risks. Employees of the cloud provider should be kept informed about these guidelines and measures for the protection of data security on an ongoing basis. All of the identified residual risks of the cloud service that could not fully be addressed should be noted by the management of the cloud provider. The cloud provider's risk assessment approach and risk assessment methodology should be documented.

When analysing risks, the following characteristics can be analysed and evaluated:

1) Evaluation of the impact on the organisation, technology, or service provision due to a security failure and consideration of the consequences of a loss of confidentiality, integrity, or availability;

2) Evaluation of the realistic probability of such a security failure, taking all conceivable threats and security gaps into account;

3) Assessment of the possible level of damage to the data subject's fundamental rights and freedoms;

4) Verification that all possible risk management options have been identified and evaluated;

5) Assessment of whether the residual risk is acceptable or if a countermeasure is required.

The data security concept should be continuously updated and improved (at least annually) in consideration of newly emerging security challenges. Risk assessments, the possible extent of damage and the identified acceptable risks should be regularly reviewed, taking technical and organisational change, identified threats, the impact of the implemented protective measures and external events into account. In addition, appropriate contacts should be established with authorities and interest groups that are relevant for the cloud provider in order to be informed at all times about current risks, threats and possible countermeasures.

Reference is made to the implementation guidance in BSI C5 OIS-03, OIS-05, OIS-06, OIS-07, SA-01, SA-02, SA-03, RB-17, SIM-01

Reference is made to the guidelines for risk management in ISO 31000, the risk assessment techniques in IEC 31010, and the guidelines for recording threats to privacy in ISO/IEC 29134.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 5.1.1, 5.1.2, 8.2, 12.1 to 12.6, 18.1, 18.2, ISO/IEC 27018 no. 5.1.1, 5.4.1 and 27701 no. 5.2.1, 5.2.2, 5.4.1, 6.3.1, 6.5.2.1, 6.5.2.2, 6.12 and 6.15.1

Determination methods

- Document review, particularly legal analysis
- Inspection
- Auditing

Determination activities

An evaluator checks the existence and contents of the data security concept through a document review. In particular, the evaluator checks in the documentation whether the risk assessment procedure is described and compatible with the GDPR, whether the risk assessment was carried out correctly and whether all identified risks (and opportunities, if applicable) are listed with a severity level for each risk. Furthermore, the evaluator checks whether trade-off analyses made by a cloud provider as part of the the risk assessment are described and whether the data security measures to address risks are specified (for example, documentation of planned measures in the company's internal ticket system and reference to risks addressed by these measures). An evaluator should also review process documents in case of risk realisation (e.g., in the form of company policies). In addition, the evaluator checks whether the area of responsibility of the cloud provider and sub-processors and cloud users are separated and adequately described in the data security concept.

An evaluator also checks the list of data categories processed by the cloud provider for consistency and completeness through a document review by randomly comparing the submitted description with the concluded commissioned processing agreements, which indicate the type of data processed on behalf of the cloud user. Through a document review, an evaluator checks whether the level of protection provided by the cloud service is adequate for the data processed on behalf of the cloud users.

As a supportive measure, interviews can be conducted within the context of an audit to check the points mentioned above for completeness and implementation in the company.

To the extent that the data security concept requires security measures to be taken by the cloud user, an evaluator checks whether these have been communicated to the cloud user in written or an electronic format. For this purpose, the evaluator examines existing protocols, contracts, process specifications for notification or other relevant documentation of the cloud provider. An interview of the responsible staff during an audit regarding the awareness of the cloud user's security measures and notification guidelines can be carried out to determine whether cloud users will also be informed in these cases in the future. If the cloud user is informed electronically, for example, within the scope of the online registration process of the cloud service, an evaluator can also check the compliant notification of the cloud user by inspection in the form of service use.

The evaluator must be able to conclude from the documents presented whether the data security concept is up-to-date and has been and continues to be further developed (e.g., through time stamps, versioning history or logs of further development). It can also be checked through interviewing or observation during an audit whether the data security concept is updated and checked for adequacy.

Furthermore, the evaluator must be able to conclude from the documents submitted that the measures implemented are state-of-the-art of technology and appropriate. The adequacy of the individual TOMs mentioned in the data security concept and their implementation are checked by an evaluator according to the following numbers of the catalogue.

No. 2.2 – Security zone and entry control
(Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

(1) The cloud provider must ensure by means of risk-appropriate TOMs that its premises and facilities are protected against damage caused by acts of god[3] and that unauthorised persons have no entry to the premises and data processing facilities so as to prevent unauthorised physical access to personal data and the possibility of manipulation of the data processing facilities.

(2) The cloud provider must control the physical entry to rooms and data processing facilities by means of a two-factor authentication procedure.

(3) The measures must be appropriate to regularly prevent unauthorised persons from obtaining entry due to technical or organisational errors, including operating errors of the cloud provider, or negligent acts of third parties. A minimum level of protection must be provided to make intentional interferences more difficult to achieve.

(4) The cloud provider must review periodically and, if necessary, update the current status and adequacy of the authorisations that are required for the entry to rooms and facilities.

Protection category 2

(5) The criteria of protection category 1 must be fulfilled.

(6) In addition, the cloud provider must take appropriate measures not only to prevent damages caused by acts of god, but also by negligent acts of authorised persons. Physical entry must be adequately protected against intentional acts of unauthorised persons, which includes protection against entry attempts by known attack scenarios, deception and force.

(7) Every unauthorised entry and entry attempt must be detectable afterwards.

Protection category 3

(8) The criteria of protection category 1 and protection category 2 must be fulfilled.

(9) Every authorised entry must be logged.

Explanation

This criterion partially substantiates the obligation contained in Art. 32 (1) lit. b) and Art. 5 (1) lit. f) GDPR, which is in need of closer definition, in more detail as regards the permanent assurance of the protection goals of availability, integrity and confidentiality (SDM C1.2 – C1.4) of personal data and services. Insofar as the cloud provider is responsible for the security zone and the entry control to the premises and data processing facilities, it will require a rights concept for the entry to data processing facilities. Entry control ensures the protection of physical access not only during normal operation but also in the context of acts of god.

Implementation guidance

Protection category 1

To ensure that unauthorised persons do not get entry to premises and data processing facilities, entry to the computing centre should be continuously monitored by video surveillance systems, motion sensors, alarm systems, and trained security staff. Entry to areas where personal data are processed should be secured with a suitable two-factor authentication procedure, e.g., consisting of an entry card and a secret PIN (s. ISO/IEC 27002 no 11.1.2). Entry rights should be reviewed and updated regularly (at least annually) and withdrawn, if necessary.

Facilities should be protected against fire, water, earthquakes, explosions, disturbances and other forms of natural hazards and human-made hazards by structural, technical and organisational measures (s. BSI C5 PS-03). These include, among other things, early fire detection and extinguishing systems, the implementation of regular fire drills and fire safety inspections to check compliance with fire protection measures, the embedding of sensors to monitor temperature and humidity and the equipping of all buildings with lightning protection devices. Expert advice can be obtained to prevent possible damage (s. ISO/IEC 27002 no. 11.1.4).

Protection category 2

The implementation guidance for protection category 1 apply.

[3] Acts of god are unusual processes occurring in nature, which cannot be influenced by humans and which last for a limited time. Examples are lightning strikes, floods, drought.

Secure protection of entry should be achieved by setting up several physical barriers around the cloud provider's premises and data processing facilities, as this way a failure of one barrier will not result in any direct impairment of data security (s. ISO/IEC 27002 no. 11.1.1).

Physical entry controls should be developed and used in particular against malicious attacks or accidents, and at the same time adapted to the technical and economic conditions of the cloud provider, which are set out in the data security concept. The building structure of the location should be physically solid, and all external doors should be adequately protected against unauthorised entry with the help of control mechanisms (e.g., barriers, alarm devices, locks) (s. ISO/IEC 27002 no. 11.1.1). Burglar-resistant material (e.g., according to DIN EN 1627 resistance class RC 2) and corresponding locking devices should be installed on the outer doors and windows (s. BSI C5 PS-01). All outer doors and all accessible windows should be monitored by burglar alarm systems.

Visitors should only be allowed supervised entry for specific purposes and only to limited areas (s. ISO/IEC 27002 no. 11.1.2). In addition, they should be instructed in the security requirements of the area concerned and in the emergency measures. All employees and external parties should be required to wear a clearly visible identification showing their entry authorisation and notify security personnel without undue delay if they encounter unaccompanied visitors or other persons who do not wear a recognisable identification.

In order to prevent malicious actions, unsupervised activities in security areas should be avoided (s. ISO/IEC 27002 no. 11.1.5). Carrying photo, video, audio and other recording devices such as cell phones should be prohibited and only permitted with explicit approval.

Reference is made to the implementation guidance in BSI C5 OIS-04, PS-01, PS-02, PS-03, PS-04.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 11.1.1, 11.1.2, 11.1.3, 11.1.4, ISO/IEC 27018 no. 11 and ISO/IEC 27701 no. 6.8 and 6.10.2

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

Access to premises and processing facilities should be documented in a physical log or an electronic audit trail, which are to be stored securely and be monitored (s. ISO/IEC 27002 no. 11.1.2). The signing in and signing out of visitors should be noted with the date and the time.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

The evaluator conducts a review of the relevant documentation on protection against damage caused by acts of god, and on access control, including the documentation of the TOM in the data security concept, business continuity concepts, authorisation concepts, and process instructions/concepts/guidelines on, for example, security guards, video surveillance, visitor regulations, intrusion detection systems, locking systems and authorisations.

The implementation of the appropriate TOM for protection against damage caused by acts of god is determined by representative random samples during an audit and checked for adequacy. The inspection and/or testing or visitation of server rooms and the assessment of measures taken (e.g., early fire detection and extinguishing systems, humidity and temperature sensors) can be carried out.

The implementation and (ongoing) operation of access controls are determined and checked for adequacy by representative random samples within the scope of inspections, tests and an on-site audit. An evaluator checks the availability and reliability of defined access controls and the awareness of instructions among employees, compares the documentation with the actual implementation of the measures on-site (e.g., security guards active, video surveillance in place, records and logs available), and conducts a walk-through of the sites. During the on-site audit, the corresponding protection category must be considered.

In support, the evaluator may perform a penetration test of access control systems or similar security tests and a check of the integration of such equipment into the security process.

Concerning the staff, an evaluator conducts document reviews and interviews as part of an audit to determine whether training and awareness-raising measures (e.g., on social engineering prevention) are carried out, to check for knowledge of appropriate rules of conduct (e.g., dealing with external persons), and to check that the documentation of measures is maintained and up-to-date (e.g., key books are up-to-date).

For protection categories 2 and 3, an evaluator shall review the process documentation for logging unauthorised access and access attempts through a document review to determine if continuous logging is being performed. Actual logging can be verified by inspection or review of access and event logs or electronic audit trails if they have

occurred. An evaluator can check whether unauthorised access and attempted access are subsequently detected as part of the on-site audit and an interview or observation of staff. For protection category 3, these checks apply analogously to determining whether each authorised access was also logged.

No. 2.3 – Admission control (Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

(1) The cloud provider must ensure that unauthorised persons are not admitted to data processing systems and that they cannot manipulate them. This also applies to backups insofar as they contain personal data.

(2) The cloud provider must periodically review the current status and adequacy of rights that are required for admission to data processing systems and update them if necessary.

(3) The cloud provider must verify the admission of authorised persons via the internet by means of a two-factor authentication procedure. Admission via the internet must be implemented through an encrypted communication channel.

(4) The measures for admission control must be appropriate to regularly prevent unauthorised persons from being admitted to data processing systems due to technical or organisational errors, including operating errors of the cloud provider, or due to negligent acts of the cloud user or third parties. A minimum level of protection must be provided to make intentional manipulations more difficult to achieve.

Protection category 2

(5) The criteria of protection category 1 must be fulfilled.

(6) Protection measures must be in place against expected intentional unauthorised admission, which are capable of excluding expected admission attempts with sufficient certainty. This includes adequate protection against known attack scenarios in particular, as well as measures by which unauthorised admissions can normally be detected (afterwards).

Protection category 3

(7) The criteria of protection category 1 and protection category 2 must be fulfilled.

(8) The cloud provider must exclude unauthorised admission to data processing systems with sufficient certainty. This includes regular measures for the active detection of attacks. Every unauthorised admission and attempt can be detected afterwards.

Explanation

The criterion of admission control partially defines the obligation contained in Art. 32 (1). lit. b) and (2) GDPR more closely, which is in need of closer definition for the permanent assurance of the protection goals of availability, integrity and confidentiality (SDM C1.2 – C1.4) of personal data and services. Insofar as the cloud provider is responsible for data processing system admission, it will require a rights concept for admission to data processing systems.

Implementation guidance

Protection category 1

Admission control rules, admission rights and restrictions should be drafted, documented, and reviewed on the basis of the risk and security-related requirements (s. ISO/IEC 27002 no. 9.1.1). Admission controls are both logical (e.g., with regard to the admission to system programs) and physical (e.g., with regard to admission to hardware interfaces) and both types must be considered together.

Admission authorisations for users under the responsibility of the cloud provider (internal and external employees) are assigned in a formal approval process with defined responsibilities (s. ISO/IEC 27002 no 9.2.2). Organisational and/or technical measures ensure that unique user IDs are assigned that uniquely identify each user (s. ISO/IEC 27002 no. 9.2.1).

Rules should be defined on the premise that basically everything is forbidden that is not expressly permitted (“Least Privilege Principle”) (s. ISO/IEC 27002 no. 9.1.1). One should only get admission to the data processing systems (IT equipment, applications, procedures, rooms) that are required for the performance of one’s own tasks/activities/functions (“need-to-know principle”).

The procedure for logging on to a system/application should be designed in such a way that the risk of unauthorised admission is as low as possible (s. ISO/IEC 27002 no. 9.4.2). The registration process should therefore reveal as little information as possible about the system/application to prevent giving any assistance to an unauthorised user. Systems should only be left after logging out or they should be protected with a screen lock and keyboard lock, which is secured by user authentication, whenever they are unattended or not used (s. ISO/IEC 27002 no. 11.2.9).

Admission rights should be reviewed on a regular basis. In particular, the admission rights of the users should be adapted when their functions or activities change. In addition, a revocation of user permissions should be carried out without undue delay when the users have left the organisation.

All of the cloud provider's facilities should be properly maintained to ensure their continued availability and integrity.

Protection category 2

The implementation guidance for protection category 1 apply.

Admission should be adequately monitored and protected to detect attacks. Among other things, virus protection and repair programs should be used, which enable signature and behaviour-based detection and removal of malicious programs (see BSI C5, beginning of RB-05).

Secret authentication details (e.g., passwords, certificates, security tokens) should be provided to employees of the cloud provider or the cloud user in a proper organised procedure, provided this is subject to the cloud provider's organisational or technical procedures, whereby the confidentiality of the information will be ensured (s. BSI C5 IDM-08. If the authentication details are initially assigned, it should only be valid temporarily, but no longer than 14 days. Users should also be forced to change these on first use. Interactive systems for managing passwords should be used, as well as strong passwords according to the state of the art (s. ISO/IEC 27002 no. 9.4.3).

A good registration process should not display any help texts that could be used by unauthorised persons during the registration process (s. ISO/IEC 27002 no. 9.4.2). The login data should only be checked after all data has been entered, and it should not be shown which part of the data entered was correct or incorrect if an error occurs. A security breach secured alert should be triggered at brute force login attempts and in the event of any detection of a potentially attempted or successful bypassing for the login control. Unsuccessful and successful login attempts should be logged. Inactive sessions should end automatically after a specified period of time.

Admission authorisation for cross-network access should be based on a security assessment on the basis of the customer requirements (s. BSI C5 KOS-03). Administrative authorisations should be checked at least every six months (s. BSI C5 IDM-05).

Reference is made to the implementation guidance in BSI C5 OIS-04, RB-05, RB-17 to RB-22, IDM-01 to IDM-13, KOS-03, KOS-04 and SIM-01 to SIM07

Reference is made to the implementation guidance in ISO/IEC 27002 no. 9, 12.1.4, 12.4.2, ISO/IEC 27018 no. 9 and ISO/IEC 27701 no. 6.6

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

Admission should be adequately monitored and protected in order to detect attacks. To this end, among other things, vulnerabilities scanners and intrusion detection, and prevention systems should be used and annual penetration tests should be carried out to identify and remedy weak points. System components that are used for the provision of the cloud service should be hardened according to the generally accepted industry standards (s. BSI C5 RB-22).

Any use of emergency users (for activities which cannot be carried out with personalised, administrative users) should be documented, justified, and made dependent on the approval of an authorised person, whose appointment is based on the principle of the separation of functions. (s. BSI C5 IDM-09). The emergency user should only be activated the duration that it is necessary to perform the relevant tasks.

The use of service programs and management consoles (e.g., for managing the hypervisor or virtual machines) that allow extensive access to the data of the cloud users should be restricted to authorised persons (s. BSI C5 IDM-12). The assignment and changes of corresponding admission rights should be carried out in accordance with the guidelines for the administration of admission rights.

Admission to service source code and associated objects (such as drafts, specifications, verification and validation plans) should be regulated and monitored in order to prevent the addition of unauthorised service functions and to avoid unintentional changes (s. ISO/IEC 27002 no. 9.4.5). This can be achieved, for example, by means of controlled central storage, preferably in software source code libraries.

Any authorised and unauthorised admission and corresponding admission attempts should be logged. The connection times should be limited to offer additional security and provide the fewest opportunities possible for unauthorised admission attempts (s. ISO/IEC 27002 no. 9.4.2).

Reference is made to the implementation guidance in ISO/IEC 29146 "Information technology - Security techniques - A framework for access management".

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

The evaluator performs a review of the access control documentation, including, for example, documentation of the TOM in the data security concept, authorisation concepts, process instructions, guidelines/concepts on passwords, documentation on authentication and encryption concepts for access (authorised employees), and on access authorisations.

The implementation and (ongoing) operation of access controls are determined within the scope of an on-site audit, inspections and testing by representative random samples and checked for adequacy according to the protection category. By interviewing the staff during the audit, it should be checked whether they are aware of appropriate rules of conduct (e.g., the prohibition of passing on passwords) and whether measures are also implemented in accordance with the documentation (e.g., checking the withdrawal of access rights after employees leave the organisation). By performing an asset test, evaluators can check access interfaces for security (e.g., blocking of employees' computers).

If remote access via the Internet is enabled, it is checked separately for security and appropriateness. Security tests (e.g., testing for encryption) can be carried out to support this.

From the documents presented, the evaluator must be able to conclude whether the access concept and the authorisations are up-to-date and continuously updated (e.g., through time stamps, versioning history or update logs). Random samples can also be taken to check the timeliness and appropriateness of authorisation. By means of interviewing or observation during an audit, it can be checked whether processes for updating access authorisations are carried out, and employees are aware of the corresponding guidelines.

For protection categories 2 and 3, an evaluator checks the process documentation for detecting unauthorised access through a document review. As a rule, the actual detection can be verified by inspection or review of access and event logs or electronic audit trails insofar as unauthorised access has occurred. As part of the on-site audit and an interview or testing, an evaluator can check whether unauthorised access can be generally detected retrospectively. For protection category 3, an evaluator checks analogously whether each unauthorised access and corresponding attempts are subsequently detectable.

No. 2.4 – Access control
(Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

(1) The cloud provider must ensure by means of TOMs that authorised persons can only access personal data within the scope of their authorisation and that unauthorised influences on personal data are excluded. This also applies to backups insofar as they contain personal data.

(2) The cloud provider must periodically review the current status and appropriateness of the rights that are required for access to personal data and update them if necessary.

(3) The cloud provider must control any access to personal data.

(4) The measures must be appropriate to regularly prevent unauthorised persons from accessing personal data due to technical or organisational errors, including operating errors of the cloud provider, or due to negligent acts of the cloud user or third parties. A minimum level of protection must be provided to make intentional manipulation more difficult to achieve.

(5) Access to personal data via the internet by authorised persons must require a two-factor authentication.

(6) The cloud provider must protect and log administrative access and activities on critical systems by means of a strong authentication mechanism. Remote administration of the cloud service by the cloud provider's employees must be done via an encrypted communication channel.

(7) If the cloud provider's employees are to have privileged access to personal data as instructed in the cloud service, this must be regulated and documented clearly. The privileged accesses must have a different user identity than the accesses for everyday work.

Protection category 2

(8) The criteria of protection category 1 must be fulfilled.

(9) Expected intentional unauthorised access must be excluded with sufficient certainty. This involves in particular adequate protection against known attack scenarios as well as measures by means of which unauthorised access can normally be detected afterwards.

(10) The cloud provider must enable the cloud user to determine different purpose-related user roles for its employees so as to exclude inappropriate access to personal data based on logics.

(11) If there is a privileged access, this access may only take place in roles that are independent from administration and data centre operation. The privileged access must be secured by means of a two-factor authentication procedure and the number of employees with privileged access must be kept as low as possible.

Protection category 3

(12) The criteria of protection category 1 and protection category 2 must be fulfilled.

(13) Unauthorised data access must be excluded with sufficient certainty. This regularly involves tamper-proof technical measures for the prevention and active detection of attacks. Any unauthorised access and related attempts can be detected afterwards.

Explanation

The criterion of access control partially substantiates the obligation contained in Art. 32 (1) lit. b) and (2) GDPR, which is in need of closer definition, in more detail as regards the permanent assurance of the protection goals of availability, integrity and confidentiality (SDM C1.2 – C1.4) of personal data and services. This requires a rights concept for access to personal data.

Technical measures are tamper-proof if they can only be changed through cooperation of several independent parties.

Implementation guidance

Protection category 1

Access rights concepts should exist for both the cloud users and the employees of the cloud provider. A formal process for the registration and deregistration of users should be implemented to enable the assignment and revocation of access rights (s. ISO/IEC 27002 no. 9.2.1). Access control rules, access rights and restrictions should be created, documented, and reviewed on the basis of the data security concept. Rules should be defined on the premise that basically everything is prohibited, which is not expressly permitted ("Least Privilege Principle") (s. ISO/IEC 27002 no. 9.1.1). One should only have access to personal data that are required to carry out one's own tasks/activities/functions ("need-to-know principle"). Access authorisations for users under the responsibility of the cloud provider (internal and external employees) should be granted in a formal approval process with defined responsibilities (s. ISO/IEC 27002 no. 9.2.2). Organisational and/or technical measures should ensure that unique user IDs are assigned that uniquely identify each user (s. ISO/IEC 27002 no 9.2.1). There should be a separation of functions between operational and controlling functions ("separation of duties") (s. BSI C5 IDM-01).

An appropriate management process for access control should be established which, in addition to checking the necessity of authorisations, also regulates the allocation, updating, control and withdrawal of authorisations, monitors and which updates access policies, and reviews password guidelines and ensures compliance.

Appropriate security measures against both internal and external attacks should be implemented to prevent unauthorised access. This includes all standard measures for protecting the cloud host, i.e. host firewalls, network intrusion prevention systems, application protection, as well as antivirus and regular integrity checks of important system files. All access to personal data should be logged.

The assignment and change of access rights for users with administrative or extensive authorisations under the responsibility of the cloud provider should take place in accordance with documented access guidelines (s. BSI C5 IDM-06). The assignment should be personalised and to the extent necessary for the performance of the task ("need-to-know principle"). Organisational and/or technical measures should ensure that the assignment of

these authorisations does not result in undesired, critical combinations that violate the principle of functional separation (e.g., assignment of authorisations for the administration of the database and the operating system). If this is not possible in selected cases, appropriate, compensatory controls should be set up to identify any misuse of these rights (e.g., logging and monitoring by a SIEM solution).

The assignment and use of privileged access rights should be restricted and controlled (s. ISO/IEC 27002 no. 9.2.3). The assignment of privileged access rights should be controlled by an official approval process. Normal business activities should not be carried out with user IDs that have privileged access rights. The competencies of users with privileged access rights should be checked regularly to ensure that they match the task profile.

Protection category 2

The implementation guidance for protection category 1 applies.

Security parameters on the network, operating system (host and guest), database and application level (where relevant for the cloud service) should be appropriately configured to prevent unauthorised access (s. BSI C5 IDM-11). The cloud service should be continuously monitored for attacks and security incidents to be able to identify suspicious activities (e.g., extraction of large amounts of data from several clients), attacks and security incidents on time and initiate appropriate and timely reactions.

So as to make it more difficult for employees to manipulate data processing operations by intent, the group of authorised persons should be kept small and access permissions must be assigned restrictively. Employees should only have access to data and data processing operations that they need to fulfil their tasks. A further measure to make intentional interference by employees more difficult can be to implement a four-eyes principle, which only permits certain actions in data processing operations if at least one other employee has agreed to the action. Accesses should be logged to be able to track accesses by authorised employees afterwards.

The process for the administration of user IDs should include the following points (s. ISO/IEC 27002 no. 9.2.1):

a) Use of unique user IDs so that users can be associated with their actions and be held responsible;
b) Regular check of access authorisations (at least annually);
c) Adaptation or deletion of user IDs and the rights of users whose functions or activities have changed;
d) Regular identification, deletion or deactivation of unnecessary user IDs;
e) Grants of privileged access rights should be checked at regular intervals to ensure that no unauthorised rights have been acquired;
f) Assurance that previously used identifiers are not assigned to other users.

Secret authentication details (e.g., passwords, certificates, security tokens) should be provided to employees of the cloud provider or the cloud user in a proper organised procedure, provided this is subject to the cloud provider's organisational or technical procedures, whereby the confidentiality of the information will be ensured (s. BSI C5 IDM-08). If the authentication details are initially assigned, it should only be valid temporarily, but no longer than 14 days. Users should also be forced to change these on first use. Interactive systems for managing passwords should be used, as well as strong passwords according to the state of the art (s. ISO/IEC 27002 no. 9.4.3).

Guidelines and instructions with TOMs for the proper use of mobile devices in the cloud provider's area of responsibility, which allow access to IT systems for the development and operation of the cloud service, should be documented, communicated and provided (s. BSI C5 MDM-01).

Reference is made to the implementation guidance in BSI C5 OIS-04, RB-05, RB-17 to RB-22, IDM-01 to IDM-13 and KOS-01, KOS-03, KOS-04, MDM-01 and SIM-01 to SIM07.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 6.2, 9, 12.4.1, 13.2, ISO/IEC 27018 no. 9, A10.13 and ISO/IEC 27701 no. 6.3.2, 6.6, 6.9.1, 6.9.2, 8.2

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

Access to personal data should be monitored and protected comprehensively to detect attacks. To this end, among other things, vulnerability scanners and intrusion detection and prevention systems should be used and annual penetration tests should be carried out to identify and remedy vulnerabilities. In addition, tamper-proof technical measures should be used to prevent and actively detect attacks. A measure is tamper-proof if, e.g., it can only be executed in interaction between the cloud user and cloud provider.

All relevant security events including all security gaps or incidents should be recorded, logged, archived and evaluated in an audit-proof manner. A capable team for security incident handling and troubleshooting should be available at all times so that security incidents can be reported and processed promptly.

Reference is made to the implementation guidance in ISO/IEC 24760-1 to ISO/IEC 24760-3.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

An evaluator reviews the documentation for access control including documentation of the TOMs under the data security concept, authorisation concepts, process instructions, regulations for privileged access, and access guidelines.

If employees of the cloud provider have privileged access to personal data on the instructions of the cloud user, an evaluator will review a representative sample of legally binding agreements with the cloud user or other documents with instructions given by the cloud user to demonstrate that the instructions are documented and regulated. Employee interviews can also be conducted as part of an audit to determine if privileged access is only assigned to roles that are independent of administration and data centre operations.

If remote access via the Internet is enabled, it is checked separately for security and appropriateness. Security tests (e.g., testing for encryption) can be carried out for this purpose. Security tests should also be carried out to check whether administrative access and activities on critical systems are sufficiently secured. An evaluator will review sample logs or database extracts to ensure that administrative access and activities on critical systems are logged.

The implementation of TOM for access control is determined during inspections, testing, and an on-site audit by representative samples and checked for adequacy according to the protection category. The inspection and testing may include, in particular, the monitoring of operations and the performance of data processing operations, and, if required, an asset test. For example, the firewall configuration, VPN accesses, teleworking stations, authentications and encryptions are to be tested. Administrative activities can also be tested, and their logging checked.

By interviewing the staff during the audit, it should be checked whether they are aware of the corresponding rules of conduct (e.g., the ban on passing on passwords) and whether measures are also carried out in accordance with the documentation (e.g., checking the withdrawal of access rights after employees leave the organisation). Remote administration by employees can also be observed on a test basis to inspect compliance with the criteria.

From the documents presented, the evaluator must be able to conclude whether the access concept and permissions are up-to-date and continuously updated (e.g., through timestamps, version history or update logs). Also, the up-to-dateness and appropriateness of authorisation can be checked on a random basis. Through interviewing or observation during an audit, it can be checked whether processes for updating access authorisations are carried out, and employees know the corresponding guidelines.

For protection categories 2 and 3, an evaluator checks the process documentation for detecting unauthorised access through a document review. As a rule, the actual detection can be verified by inspection or review of access and event logs or electronic audit trails insofar as unauthorised access has occurred. As part of the on-site audit and an interview or testing, an evaluator can check whether unauthorised access can be generally detected retrospectively. For protection category 3, an evaluator checks analogously whether each unauthorised access and corresponding attempts are subsequently detectable.

No. 2.5 – Transfer of data and transport encryption (Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

(1) The cloud provider must use state-of-the-art transport encryption or equally appropriate measures for data transfer processes or configure interfaces in such a manner that this is a requirement. The transport encryption used must ensure that personal data cannot be read, copied, modified, or deleted without authorisation during electronic transfers.

(2) The measures must be appropriate to regularly prevent attacks by unauthorised persons based on technical or organisational errors, including operating errors of the cloud provider or its employees, or negligent acts of the cloud user or third parties. Moreover, the measures must be suitable to prevent any negligent disclosure of data to unauthorised persons by the cloud provider and its employees. A minimum level of protection must be provided to make intentional interference more difficult to achieve. Whenever the transfer is encrypted, the encryption keys must be securely stored.

(3) The cloud provider must automatically log the metadata of all data transfer operations, including those of recipients and those sent from and to the cloud user or sub-processor.

(4) The requirements of this criterion also apply to the transfer of data within the cloud provider's own network and that of the sub-processor and between them.

(5) The cloud provider must protect the transport of data media with TOMs so that personal data cannot be read, copied, modified, or deleted without authorisation during transports of data media. The cloud provider must keep the records of the transports.

Protection category 2

(6) The criteria of protection category 1 must be fulfilled.

(7) The cloud provider must protect the data from intentional unauthorised reading, copying, alteration, or deleting and must exclude expected attempts with sufficient certainty. The protection measures must include adequate protection specifically against known attack scenarios and measures by which unauthorised reading, copying, alteration, or deleting can normally be detected (afterwards).

Protection category 3

(8) The criteria of protection category 1 and protection category 2 must be fulfilled.

(9) The cloud provider safely prevents unauthorised reading, copying, alteration, or deleting of data with sufficient certainty. It regularly takes measures to actively detect and deter attacks and detects any unauthorised reading, copying, alteration, or deleting of data and any attempt to do so.

Explanation

The criterion of transfer and transport control defines the obligation contained in Art. 32 (1) lit. b) and (2) GDPR more closely, which is in need of closer definition, for the permanent assurance of the protection goals of availability, integrity and confidentiality (SDM C1.2 – C1.4) of personal data and services and the protection of personal data against accidental or unlawful destruction, loss, alteration, unauthorised admission or disclosure during electronic transfer, transport, or storage on data media.

Implementation guidance

Protection category 1

Reference is made to the Technical Guidelines BSI TR-02102-2 "Cryptographic Mechanisms: Recommendations and Key Lengths. Part 2 – Use of Transport Layer Security (TLS)" in the current version. Using SSL (including version 3.0) is not a secure procedure.

Data media containing personal data should be protected from unauthorised access, misuse or falsification during transport by only using reliable transport or messenger service providers (see ISO/IEC 27002 no. 8.3.3). The transport containers should be sufficient to protect data media from environmental factors such as heat, moisture or electromagnetic fields. The data should be encrypted, and the transports and transfer times documented.

Reference is made to the implementation guidance in BSI C5 KRY-01, KRY-02, KOS-01, KOS-02, KOS-05 and KOS-07.

Protection category 2

The implementation guidance for protection category 1 apply.

Formal transfer guidelines, procedures and measures should be in place to protect the transfer of information for all types of communication systems (s. ISO/IEC 27002 no. 13.2.1). These include procedures to prevent transferred information from being intercepted, copied, changed, diverted or destroyed; procedures for the detection of and protection against malware being transferred in the use of electronic communication systems; measures and restrictions in connection with the use of communication systems, e.g., automatic forwarding of e-mails to external e-mail addresses and measures to ensure the reliability and availability of the service (e.g., measures against denial-of-service attacks).

Agreements should regulate the secure transfer of personal data between the cloud provider and external parties.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 8.3.3, 10.1.1, 10.1.2, 12.4, 13.1.2, 13.2, 14.1.3, ISO/IEC 27018 no. 10.1.1, A.10.6, A.10.9, ISO/IEC 27701 no. 6.7, 6.5.3.3, 6.10, 6.11.1.2 and 8.4.3, ISO/IEC 27040:2017-03 no. 6.7.1 and 7.7.1

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

The transfer of personal data should be comprehensively monitored and protected in order to detect attacks. To this end, for example, vulnerability scanners and intrusion detection and prevention systems should be used and annual penetration tests should be carried out to identify and remedy vulnerabilities.

Determination methods

- Document review
- Testing
- Auditing

Determination activities

An evaluator reviews the documentation on data transfer and transport encryption, including, for example, the TOM in the data security concept, process instructions, guidelines, log data, result protocols of internal/external audits, an overview of security scanners used, documentation of infrastructure access via APIs, documents on key management (especially access and storage of keys), documents on the transport of data media, and documentation of the processes for data transfer.

A comparison of the documentation with the actual implementation of the measures must be carried out. The effectiveness and timeliness of the encryption or other measures should be verified using appropriate security tests (e.g., penetration tests) or other technical means. The evaluator shall review metadata logs of all data transfer operations on a sample basis for each data transfer to the cloud user and to the sub-processor and on its own network. If data media were transported, an evaluator checks the transport logs.

An interview of employees, for example, with regard to knowledge of the relevant policies and instructions, and a sample check of the reaction of relevant employees to the implementation of defined policies and instructions should also be carried out.

For protection categories 2 and 3, an evaluator checks documentation through a document review to detect unauthorised reading, copying, modification or removal of personal data. The actual detection in the normal case can be verified by examining event logs, attack prevention and detection logs, or electronic audit trails insofar as unauthorised activities have occurred. For protection category 3, an evaluator checks analogically whether any unauthorised reading, copying, modification or removal of data and corresponding attempts are subsequently detectable.

No. 2.6 – Traceability of data processing (Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. c), e) and f) and (2) GDPR)

Criterion

Protection category 1

(1) The cloud provider must log entries, alteration, and erasures of personal data, which occur during the cloud user's intended use of the cloud service or during the cloud provider's administrative measures so as to ensure that data processing can be verified and traced afterwards. The cloud provider must observe the principles of necessity, purpose limitation, and data minimisation for the logging. It is to store the log data securely.

(2) The cloud provider must design the logs in such a way that entries, alterations, and erasures can generally be traced, even in the event of technical or organisational errors, including operating errors of the cloud provider or its employees, or in case of negligent acts of the cloud user or third parties. The cloud provider must provide a minimum level of protection against intentional manipulation of the traceability measures, which makes such manipulation more difficult.

Protection category 2

(3) The criteria of protection category 1 must be fulfilled.

(4) The cloud provider must provide protection against expected intentional manipulation of logging instances and against intentional access or manipulation of logs by unauthorised persons, whereby expected manipulation attempts are prevented with sufficient certainty. These protection measures must include adequate protection specifically against known attack scenarios and measures through which manipulation can normally be detected afterwards.

Protection category 3

(5) The criteria of protection category 1 and protection category 2 must be fulfilled.

(6) The cloud provider must prevent manipulation of the logging instances and logfiles (logs) with sufficient certainty. It regularly takes measures to actively detect manipulations and detects every manipulation and, if possible, every related attempt afterwards.

Explanation

The criterion of traceability partially substantiates the obligation contained in Art. 32 (1) lit. b) and (2) GDPR, which is in need of closer definition, in more detail as regards the permanent assurance of the protection goals of availability, integrity and confidentiality (SDM C1.2 – C1.4) of personal data and services and of personal data and services and the protection of personal data against accidental or unlawful destruction, loss, alteration, unauthorised admission or disclosure. To this end, it must be possible to check and establish afterwardswhether, when and by whom and with what effect on content, personal data have been entered, modified, or removed in data processing systems with the objective of modifying access rights for the future, if necessary. The secure retention of log data also includes ensuring that the log data can be analysed.

Because personal data are regularly collected in the course of logging, the handling of log data is also subject to data protection requirements. Reference is made to the data protection principles under Art. 5 GDPR. Particular attention should be paid to the data protection principles of data minimisation and purpose limitation under Art. 5 (1) lit. c) and b) GDPR.

Implementation guidance

Protection category 1

Logging facilities and log information should be protected against manipulation and unauthorised access (s. ISO/IEC 27002 no. 12.4.2). The measures should aim to protect against unauthorised changes being to the log information and problems in the operational process in connection with the logging facility, including:

a) changes to the types of messages recorded;
b) edited or erased log files;
c) exceeding the storage capacity of the log data media with the result that events are no longer recorded or previous events are overwritten.

The generated logs should be kept on central logging servers, where they are protected against unauthorised access and changes (s. BSI C5 RB-13). Log data should be erased without undue delay if they are no longer required for the fulfilment of the purpose.

Protection category 2

The implementation guidance for protection category 1 apply.

Authentication should take place between the central logging servers and the logged (virtual) servers to protect the integrity and authenticity of the transferred and stored information (s. BSI C5 RB-13). The transfer should be carried out using state-of-the-art encryption or via a separate administration network (out-of-band management).

Access and management of the logging and monitoring functionalities should be limited to selected and authorised employees of the cloud provider. Changes to the logging and monitoring should be reviewed and approved in advance by independent and authorised employees (s. BSI C5 RB-15).

An intrusion detection system managed outside the sphere of influence of the system and network administrators can be used to monitor compliance with system and network administration activities (s. ISO/IEC 27002 no. 12.4.3).

Reference is made to the implementation guidance in BSI C5 RB-10 and RB-11.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 12.4, ISO/IEC 27018 no. 12.4.1, 12.4.2 and ISO/IEC 27701 no. 6.9.4.

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

Access and management of the logging and monitoring functionalities should require multi-factor authentication procedure.

The availability of the logging and monitoring software should be monitored independently (s. BSI C5 RB-16). If the logging and monitoring software fails, the responsible employees should be informed immediately. The logging and monitoring software should be redundant so that logging and monitoring can also be carried out in the event of failures.

The generated logs allow a definitive identification of user access at the tenant level so as to support (forensic) analyses in the event of a security incident (see BSI C5 RB-14).

Reference is made to the implementation guidance in BSI C5 RB-13 to RB-16.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

An evaluator performs a document review by examining (in the data security concept) how a cloud provider ensures the data protection objectives by defining the subject and scope of logging, storage, integrity protection and deletion of logs, and the use of log data. Further documents can be authorisation concepts (especially user and administrator authorisations), process instructions, guidelines, log data, result protocols of internal/external audits, and risk analyses.

The implementation of this logging concept is determined by representative random samples in the course of ongoing operations and checked for adequacy. In particular, an inspection in the form of process monitoring should determine whether appropriate log entries are generated for inserting, changing and deleting personal data. By using security tests, applied protective measures of logs against manipulation can also be checked.

In addition, interviews of employees can be conducted as part of an audit to compare the measures specified in the documentation with the actual implementation of the measures.

No. 2.7For protection categories 2 and 3, an evaluator checks documentation through a document review to detect manipulation of the loggings. The actual detection in the normal case can be verified by examining event logs, attack prevention and detection logs, or electronic audit trails insofar as manipulation has occurred. For protection category 3, an evaluator checks analogically whether any manipulation and corresponding attempts are subsequently detectable. – Pseudonymisation (Art. 32 (1) lit. a) GDPR)

Criterion

Protection category 1

(1) The cloud provider must enable the cloud user to process data transferred in pseudonymised form by the cloud user.

Protection category 2 and 3

(2) If agreed with the cloud user (No. 1.7), the cloud provider must ensure that the data are processed in pseudonymised form. Pursuant to the legally binding agreement, the cloud user must pseudonymise the personal data itself or the cloud provider must conduct the pseudonymisation on the cloud user's instructions.

(3) Where the cloud provider carries out pseudonymisation, it must ensure that additional information for identifying the data subject is stored separately. The dataset with the attribution of the identifier to a person must be protected in such a way that expected manipulation attempts are prevented with sufficient certainty.

(4) If the pseudonymisation of the data on the cloud user's instructions is not effective in relation to all employees of the cloud provider, the number of privileged employees must be limited to the absolutely required minimum.

(5) If the type of processing order from the cloud user requires the de-pseudonymisation of the data, the cloud provider must ensure that the data are de-pseudonymised only on the cloud user's documented instructions.

(6) The cloud provider must guarantee that it continuously monitors technical developments in the field of pseudonymisation procedures and that its procedures comply with the current technical recommendations (best practices).

Explanation

For protection category 1, the cloud provider – insofar as it processes personal data of the cloud user – does not have to offer pseudonymisation service but it is required to maintain the pseudonymity of data when processing pseudonymised data.

In addition to encryption, pseudonymisation of personal data is explicitly mentioned in Art. 32 para.1 lit. a) GDPR as a security measure to be implemented. It contributes to assuring the protection goal of unlinkability (SDM C1.5). Pseudonymisation reduces the risks to the fundamental rights and freedoms of the data subjects because pseudonymisation prevents third parties from attaining knowledge of personal data, even if they gain unauthorised access to the cloud service, or it makes it at least considerably more difficult to identify persons,.

Implementation guidance

Protection category 1

The cloud provider should ensure by means of TOMs that a reversal of the pseudonymisation of personal data is not possible (e.g., ensuring that the cloud user's key is secret).

Protection category 2 and 3

Information on the legally compliant implementation of pseudonymisation procedures can be found in the working paper "Requirements for the Use of Pseudonymisation Solutions in Compliance with Data Protection Regulations". To monitor the pseudonymisation process, the cloud provider should appoint a suitable specialist who coordinates the consistent use of pseudonymisation and takes responsibility for important decisions.

If pseudonyms are created by means of calculation processes, they should correspond to the state of the art (e.g., BSI TR-02102-1). The separate storage of the dataset with the attribution of the identifier to a person requires a documented rights concept and access to this dataset should be restricted to an absolute minimum of trusted personnel (need-to-know principle). Each access to the dataset with the attribution should take place according to the four-eyes principle. If this is not possible, each access should be logged at the level of the individuals making the access.

To be able to carry out de-pseudonymisation in accordance with instructions, cases of wanted disclosures should be defined with the cloud user. The process of de-pseudonymisation should be logged. The log should indicate who executed the de-pseudonymisation. However, it should not contain any information that would allow conclusions as to the identifying data underlying the pseudonym.

The cloud provider should state publicly which technical standards met by its pseudonymisation procedure. For example, for pseudonymisation in medical informatics ISO 25237 can be used.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

For protection category 1, an evaluator checks documentation on the data processing process, especially concerning pseudonymised data. During an inspection, a test use of the service with pseudonymised data can be carried out, and the subsequent successful processing can be determined.

For protection categories 2 and 3, the evaluator examines the data security concept, including how pseudonymisation is performed, how identification data is stored securely and protected against manipulation, and how pseudonymised data is processed (e.g., examination of documentation of the TOM, process instructions, guidelines, log data, result protocols of internal/external audits, and the risk analysis).

The implementation of the pseudonymisation procedures is determined and checked for appropriateness for protection categories 2 and 3 within the scope of an inspection and/or test by representative samples. Likewise, the correct processing of the pseudonymous data is determined by a test. To this end, the type of programs used, the programming for pseudonymisation and their configuration should be checked as part of an asset test, and a random sample review of data records should be carried out.

A review of the effectiveness of the measures to protect the additional information for identification is also required for protection categories 2 and 3. Security tests may also be applied for this purpose (e.g., vulnerability and penetration tests).

If the nature of the contract with the cloud user requires the de-pseudonymisation of the data, an evaluator checks the legally binding agreement with the cloud user or other documents for the granting of consent by the cloud user as to whether the de-pseudonymisation is only carried out on the documented instruction of the cloud user. The evaluator performs a test to determine whether the documented instruction is complied with during de-pseudonymisation.

Interviews of employees during an audit can be conducted to compare the measures specified in the documentation with the actual implementation of the measures for protection categories 2 and 3 (e.g., compliance with guidelines and protective measures, awareness of the instructions for de-pseudonymisation).

By means of a document review (e.g., logs, versioning history), the evaluator checks for protection categories 2 and 3 whether the cloud provider continuously follows the technical development in the area of pseudonymisation procedures. This can also be determined in the context of an asset test (e.g., evidence of changes to the program code for pseudonymisation, updating of libraries, etc.). Interviews with the staff should also be conducted to check whether they are aware of and implement the current recommendations on pseudonymisation.

No. 2.8 – Anonymisation
(Art. 5 (1) lit. c) GDPR)

Criterion

Protection category 1

(1) The cloud provider must enable the cloud user to process anonymous data.

Protection category 2 and 3

(2) If agreed with the cloud user (No. 1.7), the cloud provider must ensure that the data are processed in an anonymised form. In accordance with the legally binding agreement, the cloud user must anonymise the personal data itself or the cloud provider must do so on the cloud user's instructions.

(3) If the anonymisation is carried out by the cloud provider, the cloud provider must ensure that it continuously follows the technical developments in the field of anonymisation processes, and that its processes comply with the current technical recommendations (best practices). The anonymisation according to the state of the art must prevent a re-identification of the data subject.

Explanation

For protection category 1, the cloud provider – insofar as it processes personal data of the cloud user – does not have to offer anonymisation service but it is required to maintain the anonymity of data when processing anonymised data.

Besides omitting the collecting of data, anonymisation is the most effective measure for data avoidance and data minimisation. It contributes to promoting the protection goal of data minimisation (SDM C1.1).

Implementation guidance

Protection category 1

The cloud provider should use TOMs to ensure that the anonymisation of personal data cannot be reversed.

Protection category 2 and 3

The cloud provider should state publicly which technical standards are met by its anonymisation procedure.

The cloud provider should use approved anonymisation procedures, which are suitable for the respective data processing purpose.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

For protection category 1, an evaluator reviews the documentation on the process of data processing, especially with regard to anonymous data. During an inspection, a test service use with anonymous data can be performed, and the subsequent successful processing can be determined.

For protection categories 2 and 3, an evaluator performs a document review, for example, the evaluator checks in the data security concept how the cloud provider performs anonymisation and processes anonymised data. The evaluator performs a review of the documentation on the anonymisation procedures used/offered (e.g., documentation of the TOM, process instructions, guidelines, protocol and log data, result protocols of internal/external audits and risk analysis).

The implementation of the anonymisation procedures is determined and checked for adequacy for protection categories 2 and 3 as part of an inspection and/or test by representative samples. Likewise, the correct processing of anonymous data is determined by a test. To this end, the type of programs used, the programming for anonymisation and their configuration should be checked as part of an asset test, and a random review of data records should be carried out.

Employees can be interviewed as part of an audit to compare the measures specified in the documentation with the actual implementation of the measures for protection categories 2 and 3 (e.g., questioning regarding the guidelines and regulations for anonymisation).

Through a document review (e.g., protocols, versioning history), the evaluator checks for protection categories 2 and 3 whether the cloud provider continuously follows the technical development in the area of anonymisation. This

can also be determined within the scope of an asset test (e.g., evidence of changes to the program code for anonymisation, updating of libraries, etc.). By interviewing the employees during an audit, it should also be checked whether they are aware of and implement the current recommendations on anonymisation.

No. 2.9 – Encrypting stored data (Art. 32 (1) lit. a) GDPR)

Criterion

Protection category 1

(1) The cloud provider must enable the cloud user to store encrypted data.

Protection category 2

(2) If the cloud provider stores the cloud user's personal data, the cloud provider must offer encryption procedures to enable the cloud user to store encrypted data or to encrypt the data itself on the cloud user's instructions.

(3) If the encryption of the data on the cloud user's instructions is not effective against all employees of the cloud provider, the number of privileged employees must be limited to what is absolutely necessary.

(4) The cloud provider must continuously monitor technical developments in encryption. The measures of the cloud provider must comply with the current technical recommendations (best practices).

(5) The cloud provider must continuously check the suitability of its encryption procedures and update them as needed.

(6) The cloud provider must verify the appropriate implementation of its encryption procedures by means of suitable tests and it must document them.

Protection category 3

(7) The criteria of protection category 2 apply. In addition, unauthorised access to the encryption key must be prevented with sufficient certainty by means of suitable TOMs.

(8) If the encryption is implemented by the cloud user, the cloud provider must assist the cloud user on its instructions for encrypting and decrypting data. Assistance must be given in the form of documentation and support for implementing encryption.

(9) The cloud provider must ensure that its assistance measures in the form of documentation and support for implementing encryption comply with the current technical recommendations (best practices).

Explanation

The criterion relates to the encryption of stored data, i.e. data that is idle.

For protection category 1, the cloud provider – insofar as it stores personal data of the cloud user – does not have to offer encryption procedures but it is required to maintain the encryption when storing encrypted data.

In protection category 2 and 3, the cloud provider offers encryption procedures. The encryption can be implemented by the cloud user or by the cloud provider on cloud user's instructions.

In addition to pseudonymisation, the encryption of personal data is explicitly mentioned in Art. 32 (1) lit. a) GDPR as a security measure to be implemented. The purpose of encryption is to ensure the protections goals of confidentiality and integrity (SDM C1.4 and C1.3). The threshold above which encryption is required is low, so that, personal data should be encrypted wherever possible when there is a low risk.

Implementation guidance

Protection category 1

The cloud provider should ensure by means of TOMs that the encryption of the data is maintained when it is stored in its cloud service.

Protection category 2

The state-of-the-art results from current technical standards for cryptographic procedures and their application.

Where the cloud provider encrypts the data, encryption keys should be generated in a secure environment using appropriate key generators. If possible, cryptographic keys should serve only one purpose and they should generally never be stored as a clear key type but should always be encrypted in the system. A redundant and

recoverable backup system should be used for storage to prevent the loss of a key. Keys should be changed on a regular basis. Admission to the encryption key administration system should require separate authentication. Cloud administrators should not have access to user keys.

Reference is made to the implementation guidance in BSI C5 KRY-01, KRY-03 and KRY-04.

Reference is made to the Technical Guidelines BSI TR-02102-1 “Cryptographic Mechanisms: Recommendations and Key Lengths”; BSI TR-02102-3 “Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)“; and BSI TR-02102-4 “Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Secure Shell (SSH)” in the respective current version.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 10.1, ISO/IEC 27018 no. 10.1 and 27701 no. 6.7. ISO/IEC 11770-2 contains more information on key management.

Protection category 3

The implementation guidance for protection category 2 apply. Furthermore, the cloud provider should take additional TOMs to ensure that unauthorised access to the key is adequately prevented. Access to keys should therefore be comprehensively monitored and protected. To be able to identify and fix vulnerabilities of the access to keys, for example, vulnerability scanners should be used, and annual penetration tests should be conducted.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

For protection category 1, an evaluator checks documentation on the data processing process, especially with regard to the storage of encrypted data. During an inspection, a test service use with encrypted data can be performed, and the subsequent successful storage can be determined.

For protection categories 2 and 3, an evaluator performs a document review, for example, the evaluator checks in the data security concept whether the offered and applied encryption procedures meet the current technical requirements. The evaluator performs a review of the documentation on the encryption procedures used (e.g., documentation of the TOM, process instructions, guidelines, protocol and log data, result protocols of internal/external audits, risk analysis).

The implementation of the encryption procedures is determined for protection categories 2 and 3 within the scope of an inspection and/or test by representative random samples and checked for adequacy. Likewise, the correct storage of the encrypted data is determined by a test. To this end, the type of programs used, the programming for encryption and their configuration should be checked as part of an asset test, and a random review of data records should be carried out. The implementation and security of the encryption procedures are determined by representative technical tests (e.g., penetration tests) and checked for adequacy.

Interviews of employees during an audit can be carried out to compare the measures specified in the documentation with their actual implementation for protection categories 2 and 3 (e.g., interviews with regard to the guidelines and regulations for encryption).

Through a document review (e.g., protocols, versioning history), the evaluator checks for protection category 2 whether the cloud provider continuously follows the technical development in the area of encryption and continuously checks the suitability of the procedure and updates the procedure and the documentation if necessary. This can also be determined within an asset test (e.g., evidence of changes to the program code for encryption, updating of libraries, etc.). Interviewing employees as part of an audit should also be used to check that they are aware of and implementing the current recommendations on encryption. An evaluator uses logs to check whether the cloud provider has tested the encryption techniques using appropriate technical tests.

For protection category 3, the evaluator reviews access and event logs for access to keys. An evaluator can check further documents for protection category 3, such as user documentation for encryption/decryption, documentation of encryption procedures, and protocols of meetings of a qualified IT security committee (which may be evidenced by training), in which the technical procedures for encryption/decryption are also regularly reflected.

No. 2.10 – Separate processing (Art. 5 (1) lit. b) in conjunction with Art. 24, 25, 32 para 1 lit. b) and (2) GDPR)

Criterion

Protection category 1

(1) The cloud provider must process the cloud user's data logically or physically separated from the database of other cloud users and from other databases of the cloud provider and must enable the cloud user to separate the data processing according to various processing purposes (secure client separation).

(2) Data separation must generally be maintained, even in the event of technical or organisational errors, including operating errors of the cloud provider or its employees or negligent acts of the cloud user or third parties. The cloud provider must provide a minimum level of protection to prevent intentional violations of the separation principle.

Protection category 2

(3) The criteria of protection category 1 must be fulfilled.

(4) The cloud provider must offer protection against expected intentional violations of the separation principle, in order to prevent them with sufficient certainty. The cloud provider is regularly able to detect intentional violations of the separation principle (afterwards).

Protection category 3

(5) The criteria of protection category 1 and protection category 2 must be fulfilled.

(6) The cloud provider must exclude a violation of data separation with sufficient certainty. The cloud provider must detect intentional violations of the separate processing.

Explanation

The criterion promotes the protection goals of availability, integrity, confidentiality and unlinkability (SDM C1.2 – C1.5) and therefore also aims to assure the principle of purpose limitation under Art. 5 (1) lit. b) GDPR. Secure client separation protects the data from unauthorised access, alterations, and destruction and prevents unwanted linking of the data.

Regarding the separation of the data processing according to the different purposes of the processing, it must be noted that the cloud provider merely has to offer the technical opportunity for separate processing, while the implementation of separate data processing in accordance with processing purposes is the responsibility of the cloud user.

Implementation guidance

Protection category 1

Data should be separated securely and strictly on jointly used virtual and physical resources (storage network, main memory) according to a documented concept (s. BSI C5 RB-23). A technical separation of the stored and processed data of the cloud users in jointly used resources can be achieved by means of firewalls, access lists, tagging (labelling of the data stock), VLANs, virtualisation and measures in the storage network (e.g., LUN masking).

Reference is made to the implementation guidance in BSI C5 RB-23 and KOS-05.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 12.1.4, 13.1.3 and 27701 no. 6.9.1.4.

Protection category 2

The implementation guidance for protection category 1 apply.

As relates to data storage, client-specific encryption with individual keys and the use of separate operating environments for different processing or equivalent procedures should be used. Access to data should be logged.

The cloud provider should operate technical and organisational monitoring procedures and systems to be able to detect attacks (e.g., cross-VM attacks) and malicious behaviour.

For the secure segmentation of jointly used resources for web applications, which are provided as SaaS, the session ID in the basic level should:

a) be generated randomly and have adequate entropy of at least 128 Bit (16 characters) in order to withstand educated guesses of the session ID (for example, by a brute force attack),

b) be adequately protected for transmission and client-side storage,

c) have the shortest possible limited validity (timeout), measured by the requirements for the use of the web application,

d) should be switched to a secure communication channel (HTTPS) upon successful authentication or change from an insecure communication channel (HTTP).

In case of IaaS/PaaS, the secure separation is ensured by means of physically separated networks or strongly encrypted VLANs (s. BSI C5 KOS-05).

Protection category 3

The implementation guidance for protection categories 1 and 2 apply.

The cloud provider should operate technical and organisational monitoring processes and systems to be able to identify and prevent attacks and malicious behaviour.

Determination methods

- Document review
- Testing
- Auditing

Determination activities

The evaluator conducts a review of data separation documentation, including, for example, TOM documentation, procedures, policies, internal/external audit findings, risk analyses, and service descriptions.

A comparison of the documentation with the actual implementation of the measures (e.g., separate databases) should be carried out. For this purpose, a test of the separation is suitable in the form of an asset test (e.g., of the programs used or the program code, check for separate databases) and security tests (e.g., penetration tests to determine the security level of the client separation). Interviewing relevant employees can provide further evidence (e.g., asking about guidelines, etc.).

For protection categories 2 and 3, an evaluator checks the documentation through a document review to detect intentional violations of the separation requirement. The actual detection case can be verified by reviewing event logs, protocols for defence and detection of attacks, or electronic audit trails.

No. 2.11 – Restorability after physical or technical incident (Art. 32 (1) lit. c) GDPR)

Criterion

(1) The cloud provider must ensure with risk-appropriate TOMs that the cloud service and the data are restored and made available in a timely manner after a physical or technical incident. A distinction is made between the restorability classes 1, 2, and 3:

Restorability class 1

The cloud provider must provide protection for its service against expected and probable events that is reliable enough so that these risks will not lead to a failure of the cloud service or a final loss of data in the normal course of events. Events must be expected and obvious if they are not supposed to happen but if they cannot be ruled out according to experience, despite application of sufficient caution; examples of this are traffic accidents or the technical defect of hardware.

Restorability class 2

The cloud provider must provide protection for its service against rare events that is reliable enough so that these risks will not lead to a failure of the cloud service or a final loss of data in the normal course of data processing. Events are rare if they are not supposed to happen and are unlikely according to experience, when sufficient caution is applied, but they can nevertheless occur in some cases, such as a “100-year flood” or targeted, extensive attacks on the cloud service or a sudden increase in access volume.

Restorability class 3

The cloud provider must guarantee a high level of protection for its service, which provides protection against exceptional albeit not theoretically impossible events reliably enough so that these risks will not lead to a failure of the cloud service or a final loss of data under normal data processing conditions. Events are exceptional albeit not theoretically impossible if they are not supposed to happen and do not occur according to experience, but can nevertheless occur in extremely seldom isolated cases, such as black swan events or an uncontrollable lightning strike at the data centre.

(2) The cloud provider must provide the cloud user with its concept of appropriate TOMs upon request.

Explanation

The criterion promotes the protection goal of availability (SDM C1.2). In accordance with Art. 32 (1) lit. c) GDPR, the restoring must take place "in a timely manner". What is deemed "in a timely manner" depends on the severity of the incident and the significance of the systems and data. For instance, the requirements for the restorability of data in a hospital must be stricter than in a data archive.

As the availability of personal data does not necessarily have to coincide with the data's need for protection based on the concept of protection categories, but there could be a requirement on the part of the cloud user instead for personal data of protection category 1 to be very quickly restored after a physical or technical incident, this criterion does not differentiate between protection categories.

Instead, the possibility of restorability in the restorability classes 1, 2, and 3 is expressed. Another argument in favour of differentiation is that, unlike the other criteria in number 2, restorability after a physical or technical incident does not relate to normal operations but to physical or technical incidents.

Incidents are deemed Acts of god, infrastructure disruptions and malfunctions, operating errors and intentional interference.

Implementation guidance

Restorability class 1

To restore data and systems, a cloud provider should develop an effective data backup concept that includes backup systems, restoration and mitigation plans, and a plan to periodically review and update the planned measures (s. BSI C5 RB-06). Regarding data backups, a distinction between backups and snapshots of virtual machines should be made. Snapshots do not replace backups, but they can be part of a backup strategy.

Backup copies of data, process states, configurations, data structures, transaction histories, etc. should be made on a regular basis according to a data backup concept. It should also specify retention and protection requirements. The restorability of the backup copies should be checked regularly.

The data backup strategies and measures of the data backup concept should be defined for cloud users in a transparent manner so that all information is traceable, including scope, storage intervals, storage times, and storage durations.

Reference is made to the implementation guidance in BSI C5 RB-01, RB-02, RB-04, RB-06 to RB-09.

For developing a data backup concept, reference is made to the implementation guidance in ISO/IEC 27002 no. 11.1.4, 11.2.2, 12.1.3, 12.3, 17.1.2, ISO/IEC 27018 no. 12.3.1, A.10.3 and ISO/IEC 27701 no. 6.9.1, 6.9.3, 6.13, 6.14.

Restorability class 2

For systems and services that are essential to operations, the data backup precautions should include all system information, applications and data that are required to restore the entire system in the event of damage.

As part of the operating workflows, the implementation of data backups should be monitored and measures should be defined in the event of failed planned data backups in order to ensure the completeness of the backups in accordance with the data backup guidelines (s. ISO/IEC 27002 no. 12.3.1).

TOMs for monitoring and provisioning or de-provisioning of cloud services are defined.

In addition to creating backup copies, the cloud provider should establish an emergency management system with appropriate contingency plans. Among other things, it is important to identify and evaluate possible interruptions so that plans for restoration and damage minimisation can be developed and implemented in an emergency. The contingency plans developed are to be continuously updated and tested for their effectiveness in order to ensure the fastest possible response in the event of an interruption.

Reference is made to the implementation guidance in BSI C5 BCM-01 to BCM-05.

Restorability class 3

The data backups should be kept redundantly at one or more external locations at a sufficient distance to be protected from damage at the main location (s. ISO/IEC 27002 no. 12.3.1). Data backups should be protected using state-of-the-art encryption.

Access to the backed-up data is restricted to authorised personnel (s. BSI C5 RB-06). Restoration processes include control mechanisms to ensure that restores only take place upon approval by authorised persons according to the contractual agreements with the cloud user or pursuant to the internal guidelines of the cloud provider.

Determination methods

- Document review

- Inspection
- Testing
- Auditing

Determination activities

An evaluator examines the data security concept to determine what events the cloud provider has dealt with that could lead to a physical, organisational or technical incident, whether its cloud service ensures normal, high or very high recoverability and what specific measures it has taken to ensure the recoverability of the data and the cloud service after an incident. The evaluator examines all submitted documents on data recoverability, in particular the documentation of the TOM, process instructions, guidelines, protocols for test runs of data recovery, results of internal/external audits, risk analyses, and service descriptions.

The implementation of the appropriate TOM is determined by representative samples during an audit and checked for adequacy. Interviews of relevant staff may be conducted (e.g., on knowledge of policies and procedures for recovery, etc.). Inspection and/or testing of server rooms and assessment of measures taken and techniques used for recoverability (e.g., redundant servers) should be carried out. A failure or recovery can be simulated on a test basis, and employees can be observed to check compliance with the process documentation. An evaluator also compares the duration of recovery with the duration specified in a sample of legally binding agreements with the cloud user.

The evaluator checks in the form of an inspection and/or test whether the cloud provider can make its recovery concept available to a cloud user. During an audit, employees can be interviewed about this information provision process to ensure that it is practised in the company and that all policies and process instructions are known.

No. 3 – Ensuring compliance with issued instructions (Art. 28 (3) subpara. 1 sent. 2 lit. a) and h); 29, 32 (4) GDPR)

Criterion

(1) The cloud provider must perform the Commissioned Data Processing only upon the documented instruction from the cloud user.

(2) The cloud provider must ensure by means of TOMs that the processing of the cloud user's data is only carried out on the cloud user's instructions, unless the cloud provider is obligated to process data under Union or Member State law.

(3) In the event that the cloud provider is obligated under Union or Member State law to process data, which also involves the transfer of data to a third country or an international organisation, the cloud provider must ensure by means of TOMs that it informs the cloud user of the legal requirements before the data processing, unless such law prohibits such information on important grounds of public interest.

(4) Within the framework of standardised bulk transactions, the cloud provider must guarantee the compliance with a concrete and comprehensible service description for the services it is technically able to perform, so that the cloud user can instruct the cloud provider by selecting Commissioned Data Processing. In addition, it must enable the cloud user to issue instructions by means of software orders that are automatically performed and documented.

Implementation guidance

The cloud provider is obligated under Art. 29 GDPR to train all employees with tasks relating to the processing of personal data in the contractually documented instructions. The cloud provider should also ensure compliance with the issued instructions in any data processing chain. In addition, the cloud provider should regularly verify the compliance with the cloud user's instructions.

Since compliance with instructions is essential for Commissioned Data Processing, the cloud provider should ensure this by means of TOMs. The measures should also protect against technical and organisational errors and manipulation attempts when issuing instructions. Data security measures such as admission and access control (no.2.3 and no.2.4) and ensuring the traceability of data processing (no.2.6) contribute to ensuring that instructions are followed, so that the implementation guidance given there should also be taken into account.

In practice, instructions issued by the cloud user are executed automatically, in particular by means of software commands (e.g., by interaction with a graphic user interface or via command line arguments), which is why these user interactions should also be automatically logged or documented.

The cloud provider should ensure by means of TOMs that it informs the cloud user about the legal requirements for processing, which is not subject to instructions, in fulfilment of obligations under Union or Member State law before starting the processing This ensures transparency of this processing to the cloud user, so that it can inform data subjects if necessary. According to Art. 28 (3) subpara. 1 sent. 2 lit. a) GDPR, exceptions from the requirement to provide information apply only if the law in question prohibits such information from being given on important

grounds of public interest. Examples of this are transfers by the cloud provider to investigative authorities in criminal cases, tax issues or facts relevant to state security and the secret service.

Reference is made to the implementation guidance in BSI C5 OIS-04, RB-05, RB-17 to RB-22, and KOS-01, KOS-03, KOS-04, MDM-01 and SIM-01 to SIM-07 for the protection of the cloud service from internal and external attacks and manipulations.

Reference is made to the implementation guidance in ISO/IEC 27002 no.12.2, 12.4, 12.6, 16 and ISO/IEC 27018 no. A 2.1

Reference is made to the implementation guidance in ISO/IEC 27701 no. 8.5.4.

Determination methods

- Document review, particularly legal analysis
- Inspection
- Testing
- Auditing

Determination activities

The evaluator performs a review of the documentation on the binding of instructions and checks it for legality and correctness, including, for example, documentation of the TOM, process instructions (especially for administrators), guidelines, logging of instructions, and documented measures for protection and prevention of manipulation.

In the case of individual agreements with cloud users, the evaluator carries out a random review of the legally binding agreements to compare the implementation of and compliance with the documented instructions with the actual behaviour of the employees and the cloud service. For this purpose, an inspection can be carried out by calling up an instruction as a function in the cloud service on a test basis or by instructing the relevant employees to carry out the instruction on a test basis as part of an audit.

In the case of bulk transactions, the evaluator performs an inspection in which the information in the service description on the technically executable services and instructions by software commands is compared with the actual possible interaction with a cloud service. For this purpose, the evaluator may perform service use or transaction monitoring, where instructions are executed as software commands on a test basis, and then observes the processing/result. Also, the evaluator may perform asset testing to check the implementation of possible software commands to issue instructions (e.g., source code analysis).

An evaluator also reviews sample logs of the ongoing documentation of instructions given and/or software commands issued by cloud users (e.g., log entries, timestamps, versioning of log files).

During an audit, an interview or observation of relevant employees can be carried out (e.g., for knowledge of instructions from cloud users and guidelines for compliance with these, etc.).

The evaluator will review communications made to the cloud user about legal requirements for non-directed processing to comply with legal obligations under Union or Member State law, to the extent that the evaluator has them. Evaluators may also review documentation, including, for example, documentation of the TOM or process instructions, for example, how to deal with requests from investigative authorities to release data or how to inform the cloud user of these legal requirements.

No. 4 – Reporting duty of the cloud provider

No. 4.1 – Instructions contrary to legal data protection provisions (Art. 28 (3) subpara. 1 sent. 2 in conjunction with Art. 29)

Criterion

The cloud provider informs the cloud user without undue delay if it believes that an instruction of the cloud user violates legal data protection provisions.

Explanation

It is the responsibility of the cloud user to ensure that an instruction complies with the applicable data protection law. Nevertheless, the cloud provider must not carry out an instruction indiscriminately if it doubts its lawfulness. Instead, it must warn the cloud user if it doubts the compatibility of an instruction with the applicable data protection law and await the decision of the cloud user.

Implementation guidance

If instructions are included in the legally binding Commissioned Data Processing Agreement and on issuance of every instruction after the conclusion of the agreement, the cloud provider is to consult its data protection officer if the data protection violation of the instruction becomes obvious to a cloud service employee who is trained in data protection law. The cloud provider has no obligation to review an instruction without cause.

For bulk transactions in which the cloud user instructs the cloud provider by selecting the cloud service based on a service description of the cloud provider, the cloud provider should take TOMs to inform the cloud user if the latter uses this service contrary to the service description. This includes, for example, an information text alerting the cloud user if the data security measures such as encryption and pseudonymisation provided by the cloud provider are not used.

The cloud provider should specify and document organisational processes defining contact persons, their responsibilities, procedures, and reporting channels in the event that an instruction violates data protection. These processes can be integrated, for example, in existing incident and troubleshooting management processes.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 8.2.4.

Determination methods

- Document review
- Auditing

Determination activities

An evaluator reviews documents that record how a cloud provider checks instructions, recognises doubts about their legitimacy under data protection law, and how it notifies the cloud user of this before executing the instruction. This can include documentation of the TOM, process instructions, guidelines, logging of instructions, documentation of the relevant mechanisms and reporting channels, and documented processes for checking instructions. An evaluator may also randomly examine communications that have occurred and are documented to cloud users in the event of a presumption of non-conformance.

An interview of relevant employees can be conducted as part of an audit (e.g., to gain insights about their knowledge of policies and procedural steps in case of doubt, etc.). In addition, an observation can be carried out in which a doubtful instruction is given on a test basis and the evaluator observes the process for receiving and processing the instruction.

No. 4.2 – Changes to the location of data processing (indirectly Art. 28 (3) subpara. 1 sent. 2 lit. a) and h) GDPR)

Criterion

The cloud provider must notify the cloud user without undue delay whenever the location of data processing changes from the one that is specified in the agreement (No. 1.5) during the period of validity of the agreement.

Implementation guidance

For bulk transactions, a communication process should be set up, preferably supported by an automated information system within the cloud service, for example, on the cloud provider's website, so that the cloud user knows where the data is processed in the event of a change of location.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A11.1 and ISO/IEC 27701 no. 8.5.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

An evaluator reviews the documentation of the cloud provider's information obligations (e.g., documentation of the TOM, procedures, policies, documented process for communication to the cloud user, documentation of relevant mechanisms and reporting channels). A cloud provider may also present communications that have taken place and are documented to cloud users in the event of a change of location, which is randomly checked by the evaluator.

An inspection in the form of process monitoring or an observation in the context of an audit can be used to check whether all necessary information on the change of location is communicated to the cloud user in an appropriate manner. For this purpose, a planned change of location can be simulated as a test. An interview of relevant employees can be carried out (e.g., testing their knowledge of guidelines, etc.).

No. 5 – Ensuring confidentiality among the personnel (Art. 28 (3) subpara. 1 sent. 2 lit. b) and h) GDPR)

Criterion

(1) The cloud provider must introduce an organisational process to ensure that the persons authorised to process personal data are bound by confidentiality obligations in accordance with the Commissioned Data Processing Agreement (no. 1.6), before they start the data processing activity, if they are not already subject to an appropriate, comparable legal obligation of confidentiality.

(2) The organisational process must also include the documentation of the declarations of commitment and their adjustment, if access and processing authorisations change.

Explanation

The confidentiality obligation and secrecy instruction promote the protection goal of confidentiality (SDM C1.4) (s. also no.1.6)

The confidentiality obligation applies to all employees who process personal data, irrespective of whether they process application data or master data and usage data.

Implementation guidance

The cloud provider should provide a copy of the formal obligation to its employees including information on the possible consequences of a breach of confidentiality obligations. The provider should repeat the information at appropriate intervals, e.g., in connection with training courses or when the employee's access rights and processing competences change. Furthermore, the cloud provider should regularly raise the data subjects' awareness of data protection and data security issues in relation to their activities.

The cloud provider should define in the process documentation the persons responsible for informing of obligations and fulfilling them, and when and how the information is given, which persons must be obligated and informed and at which points in time, and what evidence of the obligation and information is kept where and for how long.

Reference is made to the implementation guidance in BSI C5 KOS-08.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 7.1.2.

Determination methods

- Document review
- Auditing

Determination activities

An evaluator reviews the process documentation on the commitment to confidentiality and on the amendments of the commitments (e.g., when access and processing authorisations change). An evaluator may also conduct a review of the template of the employee confidentiality agreement document. By reviewing employment contracts with corresponding rules or additional contracts and company policies, an evaluator can randomly check the implementation of the measures.

During an audit, compliance with these requirements in all process constellations is to be verified through representative random interviews. For example, an evaluator can ask employees who are authorised to process personal data whether they have been obliged to maintain confidentiality and whether they are aware of the associated confidentiality obligations. An observation can also be made during a test change of processing rights so as to simulate the adjustments of declarations of commitment.

No. 6 – Support for the cloud user when safeguarding the rights of the data subjects

Explanation

As the controller, the cloud user is responsible for ensuring that the rights of data subjects are fulfilled. Insofar as it is not possible for it to do so, the cloud provider as the processor must provide support to it. In this case, the cloud provider must provide a point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of the data subject without undue delay.

If the data subject exercises his rights according to Art. 15 to 22 GDPR by electronic means, the information on which action is taken by the cloud user in response to the request should also be provided by electronic means if possible in accordance with Art. 12 (3) sent. 4 GDPR, unless the data subject has requested another information channel. However, it should be noted that Art. 22 GDPR is not considered in Chapter C for the AUDITOR certification.

No. 6.1 – Provision of information
(Art. 13 or 14 in conjunction with Art. 12 (1) and Art. 5 (1) lit. a) GDPR)

Criterion

(1) The cloud provider must ensure by means of TOMs that the cloud user has the opportunity to itself inform the data subject promptly about data processing in clear and simple language or arrange for this to be done by the cloud provider.

(2) The cloud provider must document instructions for fulfilling the obligation to inform.

Explanation

If personal data are collected directly from the data subject (direct collection), the cloud user is obligated under Art. 13 GDPR to inform the data subject of the circumstances of the data processing at the time when personal data are obtained. According to Art. 14 GDPR, the cloud user is also obligated to provide information if the personal data have not been obtained directly from the data subject (third-party collection). The appropriateness of the period for providing information in case of data collecting by third parties depends on the specific processing circumstances. According to Art. 14 (3) lit. a) GDPR, the period is one month after the personal data have been obtained. There are shorter periods if the personal data are used for communication with the data subject or are to be disclosed to other recipients. In the first case, Art. 14 (3) lit. b) GDPR requires the cloud user to comply with its obligation to inform at the latest on the first communication to the data subject. In the second case, according to Art. 14 (3) lit. c) GDPR, the information must be given at the latest when the data are first disclosed to the recipient.

The cloud provider must assist the cloud user in fulfilling the rights of data subjects with appropriate TOMs. This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Implementation guidance

If the cloud user itself is unable to fulfil the rights of the data subject, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of the data subject without undue delay should be provided. The cloud user's instructions can be documented by means of a ticket system.

If instructions to fulfil the obligation to inform are executed automatically (e.g., by means of software commands through interaction with a graphic user interface or by command line arguments), these user interactions should be logged automatically in order to demonstrate that the cloud provider acts in accordance with instructions.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A1.1 and ISO/IEC 27701 no. 8.3.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documents on measures taken by a cloud provider to enable the cloud user to provide information to a data subject or to have the cloud provider provide the information (e.g., mechanisms and reporting channels, service descriptions). Process documentation and protocols can also be used to verify the actual provision of information.

As part of an inspection, the evaluator can perform a trial information provision to check that this is possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support).

The evaluator should review logs of the ongoing documentation of instructions given and/or software commands issued by cloud users to implement information provision (e.g., log entries, timestamps, versioning of log files). As part of an audit, relevant employees can also be interviewed or observed (e.g., examining their knowledge of instructions from cloud users and guidelines for following them, etc.).

No. 6.2 Right of access
(Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 15 GDPR)

Criterion

(1) The cloud provider must ensure that the cloud user itself has the possibility to grant data subjects access to any data processing and provide them with a copy of the personal data or arrange for this to be done by the cloud provider.

(2) The cloud provider must document instructions on the fulfilment of the right of access.

Explanation

In accordance with Art. 15 GDPR, the cloud user is obligated to grant access to the data subject of any data processing and its circumstances upon request. The cloud provider is obligated to assist the cloud user in fulfilling the rights of data subjects by means of appropriate TOMs. This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Implementation guidance

If the cloud user itself is unable to fulfil the rights of the data subject, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of the data subject without undue delay should be provided. The instructions of the cloud user can be documented by means of a ticket system.

If instructions to fulfil the right of access are executed automatically (e.g., by means of software commands through interaction with a graphic user interface or by command line arguments), these user interactions should be logged automatically to demonstrate that the cloud provider acts in accordance with instructions.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A1.1 and ISO/IEC 27701 no. 8.3.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documentation on measures taken to provide information to a data subject or to provide information by the cloud provider. In particular, the evaluator should be given access to the documentation of the relevant mechanisms, reporting channels, and service descriptions. An evaluator should review exemplary records and logs of instructions given and subsequent information provided.

As part of an inspection, a representative sample disclosure can be carried out to check whether disclosure and provision of the data are possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). During an audit, interviews and observations can also be used to check whether information can be provided in response to a request (e.g., to gain knowledge of procedural steps, etc.).

No. 6.3 – Rectification and completion
(Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 16 GDPR)

Criterion

(1) The cloud provider must ensure by appropriate measures that the cloud user itself has the possibility to perform the rectification and completion of personal data or arrange for this to be done by the cloud provider.

(2) The cloud provider must document instructions for the fulfilment of the right to rectification and completion.

Explanation

In accordance with Art. 16 GDPR, the cloud user is obligated to rectify incorrect personal data and complete incomplete personal data upon request. The cloud provider is obligated to assist the cloud user in the rights of data subjects by means of appropriate TOMs. Rectification in accordance with Art. 16 GDPR promotes the protection goal of intervenability (SDM C1.7).

Implementation guidance

If the cloud user itself is unable to fulfil the rights of data subjects, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of data subjects without undue delay should be provided. The instructions of the cloud user can be documented by means of a ticket system.

If instructions to fulfil the right to rectification and completion are executed automatically (e.g., by means of software commands through interaction with a graphic user interface or by command line arguments), these user interactions should be automatically logged to demonstrate that the cloud provider acts in accordance with instructions.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A1.1 and ISO/IEC 27701 no. 8.3.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines the documentation of actions taken to rectify and complete data (e.g., documentation of relevant mechanisms and reporting channels, service descriptions). An evaluator should review sample records and logs of instructions given and subsequent rectifications or completions.

As part of an inspection, a representative sample rectification and completion can be carried out to check whether rectifications and completion of data are possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). During an audit, interviews and observations can also be used to check whether a correction or completion can be carried out (e.g., to gain knowledge of procedural steps, etc.).

No. 6.4 – Erasure
(Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 17 (1) GDPR)

Criterion

(1) The cloud provider ensures that the cloud user itself has the possibility to perform the erasure of personal data or arrange for this to be done by the cloud provider, so that the personal data will be erased irrecoverably and no information about the data subject can be obtained from it even when relatively great effort is involved.

(2) The cloud provider must ensure that the erasure of personal data is not only carried out in the active database but also in copies and data backups.

(3) The cloud provider must ensure that the data concerned will be erased again after a recovery of data that has previously been erased from the active database but not from the data backup yet.

(4) The cloud provider must document instructions for the fulfilment of the right to erasure.

Explanation

In accordance with Art. 17 (1) GDPR, the cloud user is obligated to erase personal data. The cloud provider is obligated to assist the cloud user by means of appropriate TOM in the exercise of the rights of data subjects. This criterion promotes the protection goals of intervenability and unlinkability (SDM C1.7 and C1.5).

Implementation guidance

If the cloud user itself is unable to fulfil the rights of data subjects, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of data subjects without undue delay should be provided. The instructions of the cloud user can be documented by means of a ticket system.

It is recommended to prepare an erasure concept, e.g., according to DIN 66398-2016. This can include the definition of erasure procedures that enable the cloud user to comply with its erasure obligations. This should include backup and fail-safe systems, including all previous versions of the data, temporary files, metadata, and file fragments.

Because Art. 17 GDPR focuses on irreversible erasure, measures of logical erasure such as the removal of personal data from directories using erasure commands are not sufficient to meet the requirements of Art. 17 GDPR.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A1.1 and ISO/IEC 27701 no. 8.3.

Since the erasure of data in backup and fail-safe systems is more time-consuming than erasure from the active database, copies and data from backup systems can also be erased at later points in time, after the erasure from the active database, e.g., in the course of overwriting or destroying the affected data media. Erasure from the backup files should generally take place no later than one year after erasure from the active database, whereas it should be aimed for shorter periods. The erasure from backup and fail-safe systems should include all previous versions of the data, temporary data, metadata, and file fragments.

The measures of DIN 66398 for creating an erasure concept can be used.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines the documentation on data erasure measures (e.g., documentation of relevant mechanisms and reporting channels, erasure concepts, service descriptions). An evaluator should review exemplary records and logs of instructions given and subsequent erasure.

Within the scope of an inspection, a representative test deletion can be carried out to check whether a (complete) erasure of data is possible (e.g., through a technical function within the cloud service or through manual requests to the cloud service support). During an audit, it can also be checked on the basis of interviews and observations whether an erasure can be executed (e.g., for knowledge of procedural steps, etc.).

No. 6.5 – Restrictions of processing (Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 18 (1) GDPR)

Criterion

(1) The cloud provider must ensure that the cloud user itself has the possibility to restrict the processing of personal data or arrange for the restriction to be implemented by the cloud provider.

(2) The cloud provider must document instructions for the fulfilment of the right to restriction of processing.

Explanation

In accordance with Art. 18 (1) GDPR, the cloud user is obligated to restrict the processing of personal data under certain conditions. The cloud provider is obligated to assist the cloud user by means of appropriate TOM in the exercise of the rights of data subjects. The criterion supports the protection goal of intervenability (SDM C1.7).

Implementation guidance

If the cloud user itself is unable to fulfil the rights of data subjects, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of data subjects without undue delay should be provided. The instructions of the cloud user can be documented by means of a ticket system.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A1.1 and ISO/IEC 27701 no. 8.3.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documentation on measures taken to restrict the processing of data (e.g., documentation of relevant mechanisms and reporting channels, service descriptions). An evaluator should review exemplary records and logs of instructions and subsequent restrictions.

Within the scope of an inspection, a representative restriction can be carried out to check whether a restriction of data processing is possible (e.g., through a technical function within the cloud service or through manual requests to the cloud service support). During an audit, interviews and observations can also be used to check whether a restriction can be implemented (e.g., to gain knowledge of procedural steps, etc.).

No. 6.6 – Notification obligation regarding rectification, erasure or restriction of processing (Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 19 GDPR)

Criterion

(1) The cloud provider must ensure that the cloud user has the possibility to notify recipients to whom it has disclosed personal data of any rectification, erasure or restriction of processing, or arrange for the notification to be given by the cloud provider and to inform the data subject of the recipients on request.

(2) The cloud provider must document instructions for the fulfilment of the notification obligation in the event of restriction, erasure or restriction of processing.

Explanation

In accordance with Art. 19 GDPR, the cloud user is obligated to inform recipients to whom it has disclosed personal data about any rectification, erasure or restriction of processing, and to inform the data subject of the recipients on request. If the cloud provider has been involved in the disclosure, it is obligated to assist the cloud user in fulfilling

of the rights of data subjects by means of appropriate TOMs. This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Implementation guidance

If the cloud user itself is unable to fulfil the rights of data subjects, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of data subjects without undue delay should be provided. The instructions of the cloud user can be documented by means of a ticket system.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A1.1 and ISO/IEC 27701 no. 8.3.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documentation on communication actions (e.g., documentation of relevant mechanisms and reporting channels, service descriptions). An evaluator should review exemplary records and logs of instructions given and subsequent communication.

During an inspection, a representative instruction to notify can be carried out to check whether notification is possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). In the context of an audit, interviews and observations can also be used to check whether a notification instruction can be carried out (e.g., to gain knowledge of procedural steps, etc.).

No. 6.7 – Data transmission
(Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 20 (1) and 2 GDPR)

Criterion

(1) The cloud provider must ensure that the cloud user has the possibility to transmit the personal data provided by a data subject to this person or another controller in a structured, commonly used and machine-readable format, or to arrange for it to be transmitted by the cloud provider.

(2) The cloud provider must document instructions for the fulfilment of the right to data portability.

Explanation

In accordance with Art. 20 (1) and 2 GDPR, the cloud user is obligated, at the request of the data subject, to transmit the provided personal data in a structured, commonly used and machine-readable format to the data subject or another controller. To assure clarity in this respect, the cloud provider should list the commonly used formats it can use in the legally binding agreement.

The cloud provider is obligated to assist the cloud user in the fulfilment of the rights of data subjects by means of appropriate TOM. The criterion promotes the protection goal of intervenability (SDM C1.7).

Implementation guidance

The cloud provider should provide appropriate technical functions within its offered service that allow it to transmit data in a structured, commonly used and machine-readable format. These include, for instance, export functions into XML or JSON formats.

If the cloud user itself is unable to fulfil the rights of data subjects, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of data subjects without undue delay should be provided. The instructions of the cloud user can be documented by means of a ticket system.

Reference is made to the implementation guidance in BSI C5 PI-01 to PI-04.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A1.1, A9.3 and ISO/IEC 27701 no. 6.5.3.3, 8.3.

Reference is made to the implementation guidance of ISO/IEC 19941 on portability.

Determination methods

- Document review
- Inspection

- Auditing

Determination activities

The evaluator reviews documentation on data transfer actions (e.g., documentation of relevant mechanisms, export formats, service descriptions). An evaluator should review exemplary records and logs of instructions given and subsequent data transfer.

Within the scope of an inspection, a representative data transmission with test data can be carried out to check whether transmission of the data is possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). During an audit, evaluators can interview and observe employees to check whether a data transfer can be carried (e.g., to gain knowledge of procedural steps, etc.).

No. 6.8 – Objection
(Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 21 (1) and Art. 32 (1) lit. b) GDPR)

Criterion

(1) The cloud provider must ensure that it provides the cloud user with all data that are necessary for it to assess whether the right of the data subject to object has been effectively exercised.

(2) If the objection to the data processing is effective, the cloud provider must ensure within the limits of its abilities that the data can no longer be processed.

(3) The cloud provider must document instructions for the fulfilment of the right to object.

Explanation

In accordance with Art. 21 GDPR, the data subject has the right to object to processing of personal data relating to him. Where the data subject has effectively exercised the right to object, the cloud user is obligated to refrain from processing the personal data of the data subject in the future. The cloud provider is obligated to assist the cloud user in fulfilling the rights of data subjects by means of appropriate TOMs. Therefore, the cloud provider must provide the cloud user with all information available to it so that the cloud user is able to make the assessment. The criterion promotes the protection goal of intervenability (SDM C1.7).

Implementation guidance

The cloud provider should have a policy in place defining the measures it takes to ensure that it can provide the cloud user with all the necessary data and prevent future processing of the data.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A1.1 and ISO/IEC 27701 no. 8.3

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documentation on measures for receiving objections and termination of processing (e.g., documentation of relevant mechanisms and reporting channels, service descriptions). An evaluator should review exemplary records and logs of instructions given and, where applicable, subsequent termination of processing. It should also be checked that there are no further logs of processing after termination (e.g., further accesses to data within an access log) to ensure that the processing has been terminated.

As part of an inspection, a representative objection can be conducted to check whether the cloud provider can provide all data to the cloud user for decision making and, if necessary, whether termination of processing is possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). In the context of an audit, interviews (e.g., to gain knowledge of procedural steps, etc.). and observations can also be used to check whether and how an objection instruction can be carried out. Similarly, an evaluator checks whether a cloud provider provides the cloud user with all the data necessary to enable the cloud user to assess whether the data subject's right to object has been effectively exercised.

No. 6.9 – General obligation to inform and obligation to inform in the event of inaction or delayed request processing
(Art. 12 (3) and (4), Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 15 to 21 GDPR)

Criterion

(1) The cloud provider must ensure by means of TOMs that the cloud user has the possibility to inform the data subject on actions taken pursuant to Art. 15 to 21 GDPR on his request without undue delay, whereas at the latest within one month after receipt of the request. Alternatively, the information can be provided by the cloud provider.

(2) The cloud provider must ensure by means of TOMs that the cloud user has the possibility to inform the data subject if it does not answer to his request pursuant to Art. 15 to 21 GDPR without undue delay, whereas at the latest within one month after receipt of the request. The information refers to the extension of the period and the reasons for an extension. Alternatively, the information can be provided by the cloud provider.

(3) The cloud provider must ensure by means of TOMs that the cloud user has the possibility to inform the data subject at the latest within one month from his request, if it does not take action to answer to his request pursuant to Art. 15 to 21 GDPR. The information of the data subject must relate to the reasons for the inaction of the cloud user and the possibility to lodge a complaint with a supervisory authority and seek a judicial remedy. Alternatively, the information can be provided by the cloud provider.

Explanation

According to Art. 12 (3) sent. 1 GDPR, the cloud user must provide the data subject with the necessary information on actions taken upon his request pursuant to Art. 15 to 22 GDPR, without undue delay, whereas at the latest within one month after receipt of the request. Art. 22 GDPR is not considered in Chapter C in the AUDITOR certification. The cloud user must therefore comment on the requested action upon every request from a data subject in accordance with Art. 15 to 21 GDPR. If the cloud user relies on a (national) exception from the rights of the data subject when answering requests, it shall therefore provide an adequate explanation to the data subject of the reasons for rejecting his request in part or in full.

Due to the complexity or the number of the requests, the one-month period from Art. 12 (3) sent. 1 GDPR can be extended by two months. In this case, the cloud user must inform the data subject of the extension of the period and the reasons for the extension according to Art. 12 (3) sent. 3 GDPR. The cloud provider must support the cloud user for this purpose. If the request is made by electronic means, the information should also be provided by electronic means, unless requested otherwise by the data subject.

Art. 12 (4) GDPR requires the cloud user to inform the data subject, at the latest within one month, of the reasons why it will not do anything to comply with the request in spite of a request received pursuant to Art. 15 to 21 GDPR. Reasons not to comply with a request are, e.g., unfounded or excessive requests according to Art. 12 (5) sent. 2 lit. b) GDPR. Furthermore, according to Art. 12 (4) GDPR, the data subject must be informed of its option to lodge a complaint with the supervisory authority according to Art. 77 GDPR or seek a judicial remedy according to Art. 79 GDPR.

Implementation guidance

If the cloud user itself is unable to fulfil the rights of data subjects, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of data subjects without undue delay should be provided. The instructions of the cloud user can be documented by means of a ticket system.

If instructions to fulfil the obligation to inform are implemented automatically (e.g., by means of software commands through interaction with a graphic user interface or by command line arguments), corresponding fields should also be provided where the cloud user can enter information about the action taken, the extension of the period, and the reasons for this or the reasons for its inaction, and the possibility to lodge a complaint with the supervisory authority or seek a judicial remedy. These user interactions should be logged automatically to demonstrate that the cloud provider acts in accordance with instructions.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documents on measures taken by a cloud provider to enable the cloud user to provide information to a data subject or to have the cloud provider provide the information (e.g., mechanisms and reporting channels, service descriptions). Process documentation and protocols can also be used to check the provision of information, including the completeness of the information provided and its timely provision.

As part of an inspection, the evaluator can perform a trial provision of information to check that it is possible (e.g., through a technical function within the cloud service or through manual requests to cloud service support) and provides all the required information.

The evaluator should review logs of the ongoing documentation of instructions given and/or software commands issued by cloud users to implement the provision of information (e.g., log entries, timestamps, versioning of log files). During an audit, an interview (e.g., examining their knowledge of instructions from cloud users and guidelines for following them, etc.) or observation of relevant employees can also be carried out.

No. 7 – Assistance in data protection impact assessment (Art. 28 (3) subpara. 1 lit. f) in conjunction with Art. 35 and 36 GDPR)

Criterion

(1) The cloud provider must assist the cloud user in the performance of its data protection impact assessment.

(2) If the cloud provider is aware of a high risk of processing due to a data protection impact assessment carried out beforehand by the cloud user, the cloud provider must take precautions as appropriate to the risks.

(3) The cloud provider must provide the cloud user with all information falling within its area of responsibility, which the cloud user requires for its data protection impact assessment.

(4) The cloud provider must assist the cloud user in counteracting risks by corrective measures planned by the cloud user including security precautions and other processes, for example, which serve to ensure the protection of personal data.

Explanation

If the cloud user is obligated to prepare a data protection impact assessment, the cloud provider must assist it by means of information, analyses and protective measures.

Implementation guidance

The obligations to assist in the data protection impact assessment should be oriented on the cloud provider's sphere of influence, e.g., as part of TOMs to ensure data security. Data flow models and analyses can be prepared to assess whether there is a risk in the respective data processing operations of the cloud service and, if so, what the risk is, if this is not already apparent from the cloud provider’s service description.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 18.1 and ISO/IEC 27701 no. 8.2.5.

Reference is made to the implementation guidance in ISO/IEC 29134 on data protection impact assessment.

Determination methods

- Document review
- Auditing

Determination activities

An evaluator should review the documentation on information obligations, including cloud user assistance documents (e.g., service descriptions, TOMs, data flow models and analyses), performed data protection impact assessments and corresponding meeting minutes, documentation of precautions taken, procedure directories, process instructions, and policies. In particular, the evaluator must ensure during the document review that the necessary information is available or can be generated by the cloud provider within a short period of time.

A comparison of the documentation and legally binding agreement with the actual implementation of the measures must be carried out. Interviews with relevant employees during an audit is necessary (e.g., questioning their knowledge of guidelines, etc.). Observation can be used to check whether and how employees process a test request from a cloud user for a data protection impact assessment.

Chapter III: Data protection management system of the cloud provider

Explanation

The cloud provider must organise its data protection measures in a data protection management system. The establishment of a data protection management system is mentioned in Articles 24, 25, 32, 33, 34 and 37 to 39 GDPR. The assurance of a data protection management system should support the constant assurance of the data protection level of the certified cloud service.

No. 8 – Data protection management system

No. 8.1 – Designation, position, and tasks of the data protection officer (Art. 37 to 39 GDPR, Sec. 38 (1) and (2) in conjunction with Sec. 6 (5) sent. 2 BDSG)

Criterion

(1) If the cloud provider is obligated to designate a data protection officer (DPO), it must appoint one based on his professional qualities and expert knowledge of data protection law and practices, and based on his ability to fulfil the tasks referred to in Article 39 GDPR.

(2) The cloud provider must ensure that the DPO reports directly to the highest management level.

(3) The cloud provider must ensure that the DPO does not receive any instructions concerning the performance of tasks in the exercise of his duties.

(4) The cloud provider must ensure that the DPO is properly involved, early on in all issues relating to the protection of personal data.

(5) The cloud provider must ensure the person and function of the DPO is recognised in the organisation structure and it must support him in the performance of his tasks, in particular by making appropriate resources available.

(6) The cloud provider must ensure that the DPO carries out his tasks in accordance with Art. 39 (1) GDPR to a suitable extent.

(7) The cloud provider must ensure that the DPO is bound to maintain secrecy or confidentiality in the performance of his tasks and beyond the end of his legal relationship with the cloud provider. This includes in particular the duty of the DPO to maintain secrecy concerning the identity of data subjects and circumstances making data subjects to be identifiable, unless he is released from this obligation by the data subject.

(8) The cloud provider must publish the contact details of the DPO and communicates this data to the supervisory authority.

(9) The cloud provider must ensure that other tasks or duties of the DPO do not lead to a conflict of interest with his activity as DPO.

Explanation

If cloud providers are obligated to designate a DPO, they must carefully select, equip, and protect him, and allocate him the place he merits within the company organisation. Art. 38 (5) GDPR stipulates that the DPO is bound by secrecy or confidentiality in the performance of his tasks. The legal norm is to be interpreted to the effect that this obligation continues to apply to the DPO beyond the end of his legal relationship with the cloud provider.

If a DPO is designated, the DPO must comply with his legal obligations with respect to all data processing operations performed, regardless of whether the cloud provider is acting as processor or controller.

Implementation guidance

The cloud provider should maintain written documentation of the systems, procedures and processes (software, hardware, involved organisational units, roles, and service providers) used for the cloud service in question and provide as accurate a description as possible of all TOMS put in place (e.g., in a data security concept), and make this available to the DPO and, upon request, to the supervisory authority.

If the DPO is employed by another company (external DPO of the cloud provider) or if he is simultaneously also the DPO of other companies, the DPO's independence from instructions also applies to its employer and other clients. The requirement of the absence of conflicts of interest is primarily a designation requirement and, in a secondary respect, an organisational obligation of the cloud provider. The cloud provider does not assign additional tasks to the DPO which could result in a conflict of interests. Conflicts of interest are to be assumed present in the course

of the following activities: activities within the scope of which the DPO would have to monitor himself, e.g., position as a managing director, IT or HR manager, economic interests of the DPO in the success of the company or in too close a proximity to the designating body.

The DPO's obligation of secrecy or confidentiality includes all relevant information in this regard. This should also be evident from the designation certificate. The DPO is also obligated to maintain confidentiality in relation to the designating body. The criterion promotes the protection goal of confidentiality (SDM C1.4).

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.3.1.

Determination methods

- Document review, particularly legal analysis
- Auditing

Determination activities

An evaluator checks internal and also external documents to determine the appointment of the DPO and the publication of his contact details. External documents can be, for example, the imprint or the privacy statement on the cloud provider's website. However, as these details may be optional, internal documents such as the confirmation of a successful notification of the DPO to the supervisory authority; the job description of the DPO; certificates of appointment; certificates of professional competence (e.g., certificates of persons, training certificates); task and procedure descriptions; guidelines; organisational chart describing the classification of the DPO; provision of staff awareness protocols on the role of the DPO; interview protocols with DPOs to verify compliance; and activity reports should be a suitable means to verify the actual appointment.

In addition, an interview with the DPO and other employees of the company during an audit should be used to verify the appointment of the DPO and the awareness of the DPO within the company.

To verify the professional qualification of the DPO, the cloud provider submits relevant documents leading to the proof of expertise to the evaluator for document review. This includes a current signed CV of the DPO listing all relevant points that demonstrate relevant expertise with regard to the topic of data protection. Furthermore, the qualification of the DPO can be proven by certificates (studies or comparable) or confirmations of participation in data protection-relevant courses/training. An interview with the DPO during an on-site audit can also provide information about the suitability and position of the DPO.

Regular internal audits of the DPO can provide evidence of his activities, his independence and his integration and effectiveness in the organisational structure of the cloud provider. For this purpose, corresponding audit protocols should be reviewed. Through an interview, the DPO is asked about the recognition and functions of his position as DPO. In addition, documents that prove the hours worked in the DPO's field of activity can be consulted. Furthermore, documents showing employer-sponsored training on data protection issues can provide evidence about the organizational support by the cloud provider. An on-site audit can determine whether the DPO has the necessary equipment and support.

The addressees of the DPO's reports (e.g., reports of data protection breaches) should be determined by document review. For this purpose, internal documents or e-mails that the DPO wrote can be used as a basis. The addressees must be at the highest management level according to the organisation chart or comparable indications. By interviewing the management, it can be checked whether the DPO reports directly to them.

In order to assess the confidentiality obligation, an evaluator can check the relevant signed appointment document of the DPO with the required contents as part of a document review and interview the DPO about his confidentiality obligation.

The evaluator interviews the DPO regarding involvement in issues that have an impact on the protection of personal data. In addition, minutes of relevant meetings, for example, may provide evidence of the DPO's presence and involvement.

Through an interview, the DPO is asked about his or her tasks in order to exclude the possibility of a conflict of interest. In addition, documents proving the hours worked in the DPO's field of activity can be consulted. In order to check for possible conflicts of interest, the availability of resources, interviews with relevant staff members and inspection of documentation of relevant mechanisms and reporting channels can be carried out. Through an interview, the DPO is asked about the authority of superiors or other employees in the context of his or her activities as DPO. Regular internal audits of the DPO can provide evidence of his activities, his independence and his integration and effectiveness in the organisational structure of the cloud provider. For this purpose, corresponding audit protocols should be reviewed.

No. 8.2 – Notification of personal data breaches
(Art. 33 (2) and Art. 28 (3) subpara. 1 sent. 2 lit. f) GDPR)

Criterion

(1) The cloud provider must ensure by appropriate measures that it notifies personal data breaches and their extent to the cloud user without undue delay.

(2) The cloud provider must determine who is responsible for deciding on and carrying out the notification to the cloud user. The competent authorities must be accessible to employees and sub-processors in such a way that notifications of possible violations can be received and processed promptly.

(3) The competent authorities must have sufficient resources to ensure that notifications are processed without undue delay. The employees in the responsible departments must be sufficiently trained to be able to assess violations and carry out an impact assessment.

Explanation

Pursuant to Art. 33 (2) GDPR, the cloud provider is obligated to notify data protection violations to the cloud user without undue delay so that the cloud user can comply with its notification obligation toward the supervisory authority under Art. 33 (1) GDPR and its obligation to communicate the violation to the data subjects under Art. 34 (1) GDPR. This obligation also applies to violations at sub-processor violations throughout the sub-processing chain. The criterion promotes the protection goal of integrity and transparency (SDM C1.3 and C1.6).

Implementation guidance

The cloud provider should establish and document corresponding processes, and define contact persons, responsibilities and reporting channels. Personal data breaches can be notified using appropriate information systems within the service, such as messaging systems or news messages. The notification of personal data breaches should be integrated into the incident and troubleshooting management of the cloud provider to enable timely processing.

Reference is made to the implementation guidance in BSI C5 SIM-01 and SIM-07.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 16.1.1, 16.1.2, ISO/IEC 27018 no. A 9.1 and ISO/IEC 27701 no. 6.13.1, 8.2.5 and 8.3.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

An evaluator examines the data security concept and the TOMs described therein to ensure the notification of data protection breaches. The evaluator may also examine further documentation on the cloud provider's information and notification obligations, including, for example, process documentation for information to users, procedure directories, procedure instructions, guidelines and training documents.

The implementation of this concept can be checked by an inspection or observation of a sample message to an evaluator as a simulated cloud user. Similarly, it should be checked whether a data protection breach notification is possible on a test basis by an evaluator and whether breaches are received and processed promptly. Logs of past communications to the user can also be reviewed. In the context of an on-site audit, it should be checked whether sufficient resources are available to ensure that messages are processed quickly.

As part of a document review, the evaluator should also check that the cloud provider has contractually committed to reporting data breaches to the cloud user. For this purpose, the provisions in the template contracts or concluded contracts should be examined on a sample basis (see also No. 1.7).

The competence of the employees should be verified by checking the documentation of skills (e.g., certificates) or training courses and by employee interviews. The evaluator can also check the organisation chart or an overview of the staff responsibilities with corresponding documented staff qualifications. In doing so, the evaluator must also check through interviews whether responsibilities are clearly communicated and regulated (e.g., who is responsible for deciding on and making the notification to the cloud user).

No. 8.3 – Maintaining a record of processing activities (Art. 30 (2) to (5) GDPR)

Criterion

(1) If the cloud provider is obligated to maintain a record of processing activities, it must list all categories of processing it performs on behalf of cloud users. The record must contain the content listed in Art. 30 (2) lit. a) to d) GDPR.

(2) The cloud provider must maintain processes for updating the records of processing activities if new categories of processing it performs on behalf of the cloud user are introduced or discontinued, or if the information according to Art. 30 (2) lit. a) to d) GDPR for listed categories of processing changes or for existing cloud users on whose behalf processing activities are carried out, added or discontinued.

(3) To be able to update the record of processing activities, the cloud provider must have processes for cooperation between the specialist departments involved in the processing, the cloud users on whose behalf processing activities are carried out and their representatives and, if applicable, the DPOs of the cloud users, and must regulate the internal responsibilities for this purpose.

(4) The record of processing activities must be kept in writing or in an electronic form and the locations where the record is retained or stored must be known.

(5) The record of processing activities must be made available to the supervisory authority upon request. The cloud provider must have processes for receiving, processing and answering requests from supervisory authorities and regulate the internal responsibilities for this purpose.

(6) If the cloud provider is obligated to designate a representative and maintain a record of processing activities, it must ensure that the representative also keeps the record of processing activities and complies with the criteria according to (1) to (5).

Explanation

The criterion promotes the protection goal of transparency (SDM C1.6).

Controllers and processors with more than 250 employees are generally obligated to maintain records of processing activities. However, even if the cloud provider has fewer employees, it must maintain a record of processing activities if the processing it carries out is likely to result in risks to the rights and freedoms of data subjects in accordance with Art. 30 (5) GDPR, or it processes special categories of data in accordance with Art. 9 or 10 GDPR or the processing is performed not merely occasionally.

According to Art. 30 (2) GDPR, the representative of the cloud provider, if one is designated, must also maintain records of processing activities (s. no. 11.2).

Implementation guidance

For standardised bulk transactions, the records of processing activities should be created automatically. Various system tools for this purpose are already commonly available on the market.

The record of processing activities can be used to demonstrate or confirm compliance with all documentation obligations. This record is not public, however, and is not directed at data subjects but is exclusively used internally and in the relationship with the supervisory authority.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 18.1, ISO/IEC 27018 no. A 5.2 and ISO/IEC 27701 no. 8.2.6,

Determination methods

- Document review
- Auditing

Determination activities

An evaluator checks the submitted processing directories for completeness, form (written or electronic format) and timeliness (e.g., timestamp, versioning history). If a standardised agreement has been concluded with the cloud user, the evaluator checks the underlying standardised processing directory. If no standardised agreements have been concluded with a cloud user, an evaluator checks all or a representative sample of processing directories of cloud users as part of the document review. A representative sample should be chosen at least broad enough to ensure that a comparative review of a selection of directories and agreements is highly likely to rule out the possibility that another directory is inadequate. The sample size is therefore also dependent on the total number of directories. The individual directories can be combined into groups, whereby a sufficient number of directories from each group of directories must be checked. Directories can be grouped according to, among other things, the subject matter, the duration, the nature and the purpose of the processing.

An evaluator checks the process descriptions of the cloud provider with regard to the procedure and completeness of the conditions in which processing directories require an update.

An evaluator checks the cooperation of the relevant stakeholders for the processing directory within the scope of a document review. For this purpose, the evaluator may examine process descriptions, organisational charts, task distribution plans or other documents.

Through a document review, an evaluator examines the processes for receiving, handling and responding to requests from supervisory authorities related to processing directories. For this purpose, the evaluator may examine process descriptions, organisation charts, task distribution plans or other documents.

In support of this, an evaluator can conduct interviews with employees as part of an audit in order to check the directories for completeness and up-to-dateness and to assess whether the cooperation of the relevant stakeholders for the processing directory takes place in accordance with the process description and whether the storage locations of the processing directories are known.

If the cloud provider states that it is not obliged to maintain processing directories due to Article 30 (5) GDPR, the evaluator will conduct an interview or document review to determine the number of employees of the cloud provider as part of an audit. The evaluator examines whether the processing of the cloud provider poses a risk to the rights and freedoms of the data subjects, the processing is not only carried out on a routine basis, or special categories of data are processed in accordance with Art. 9 or 10 GDPR, which oblige the cloud provider to keep of a processing directory, despite a number of employees of less than 250. For example, the evaluator reviews the documentation of the risk assessment in the context of Art. 24, 25 or 32 GDPR or the concluded contracts in accordance with Art. 28 GDPR.

No. 8.4 – Return of data media and erasure of data (Art. 28 (3) subpara. 1 sent. 2 lit. g) and h) GDPR)

Criterion

> The cloud provider must ensure by appropriate measures that the return of provided data media, the return of data, and erasure of data stored by the cloud provider take place after the completion of the processing on the behalf of the cloud user or upon instruction by the cloud user, unless Member State or Union law prescribe an obligation for the storage of the personal data.

Implementation guidance

It is recommended to create an erasure concept, e.g., according to DIN 66398-2016. This can include the establishment of erasure procedures that enable the cloud user to comply with its erasure obligations. The erasure concept should also include backup and fail-safe systems, including all previous versions of the data, temporary files, metadata, and file fragments.

Since the erasure of data in backup and fail-safe systems is more time consuming than erasure in the active database, copies and data from backup systems can also be erased at later times than in the active database, e.g., in the course of overwriting or destroying the affected data media. Erasure in the backup files should take place usually no later than one year after erasure from the active database, whereas shorter periods should be aimed for. Erasure in backup and fail-safe systems should include all previous versions of the data, temporary data, metadata, and file fragments.

Because Art. 17 GDPR relates to irreversible erasure, measures for logical erasure, such as the removal of personal data from directories using erasure commands, are not sufficient to meet the requirements of Art. 17 GDPR. Erasing linkings or links to data records is not sufficient either, since the data records continue to exist. The methods used for data erasure (e.g., by repeatedly overwriting the data) should prevent a recovery by forensic means.

All data media of the cloud provider should be disposed safely and securely in accordance with a formal management process after the commissioned data processing agreement has ended or when accordant instructions are given by the cloud user. Guidelines and instructions should take the following aspects into account (see ISO/IEC 27002 no. 8.3):

a) Secure and irrevocable erasure of data and disposal/destruction of data media,
b) Encryption of removable media,
c) Transfer of data to new data media when a medium is replaced.

The measures of DIN 66398 for creating an erasure concept, and of DIN 66399 and ISO/IEC 21964-1 for the destruction of data media can be used.

Reference is made to the implementation guidance in BSI C5 AM-04, AM-07, AM-08 and PI-05.

Reference is made to the implementation guidance for data erasure in ISO/IEC 27002 no. 11.2.7, ISO/IEC 27040-03 no. 6.8.1, ISO/IEC 27018 no. A 9.3 and ISO/IEC 27701 no. 6.5.3, 6.5.3.3, 6.8.2.7, 8.4.2.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

An evaluator performs a document review, including reviewing process instructions and policies for the release of data media, for the return and deletion of data after completion of the order (e.g., documentation of the TOM, data deletion concepts, procedure directories, process documentation for data (or data carrier) handling, process instructions, policies, documented instructions). An evaluator can also check the acknowledgement of returns or the automated notification of deletions of personal data no longer required for the commissioned processing.

An inspection and/or test (e.g., source code analysis, analysis of databases) or test deletion and return can be used to determine whether a return and deletion of the personal data takes place after the completion of the commissioned processing or according to the instructions of the cloud user. Interviewing relevant employees (e.g. for their knowledge of policies etc.) during an audit can lead to further information and insight into the implementation of the measures.

Supporting security tests can be conducted to verify that data has been deleted in a sufficiently secure manner.

No. 8.5 – Establishing an internal control system (Art. 24 GDPR)

Criterion

(1) The cloud provider must review the implementation of all criteria examined in this catalogue regularly in an internal audit procedure. For this purpose, the cloud provider must define control procedures and responsibilities.

(2) The cloud provider must ensure, with appropriate TOMs that the criteria examined in this catalogue continue to be observed during the (further) development or change of the cloud service.

Explanation

The cloud provider must ensure that the measures to fulfil legal data protection obligations in accordance with this catalogue are not just implemented once but maintained throughout the validity period of a certificate.

Implementation guidance

The cloud provider should use the internal audits of the DPO to address data protection issues. Moreover, reference is made to the implementation guidance for regular review by the cloud provider's top management under ISO/IEC 27002:2017-06, no. 18.1 and no. 18.2.

The cloud provider should regularly review the effectiveness of internal control activities. The first step is to define how the effectiveness of internal control activities can be measured. It is recommended to define and observe a standardised process model (such as ITIL or COBIT) for the IT processes of the offered cloud service. If an internal auditor is used, he/she should be suitably qualified, objective and impartial, and not involved in the preparation of the items to be audited.

When providing a cloud service, processes for secure change management and release management should be established. As part of these processes, the cloud provider should conduct a documented proficiency test and acceptance process in the (further) development and modification (in particular, patches and system updates) of its service so as to avoid adverse effects due to the modifications and to continuously ensure compliance with the General Data Protection Regulation. The scope, roles, and responsibilities of change and release management should be clearly defined and aligned between cloud providers and cloud users.

Reference is made to the implementation guidance in BSI C5 BEI-01 to BEI-12 with regard to the embedding of the audit process in the change management and SPN-01 to SPN-03, COM-02 and COM-3.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 5.1.2, 9.2.5, 14.2.3, 15.2.1 and ISO/IEC 27701 no. 5.7, 6.9.7, 6.15.

Determination methods

- Document review
- Auditing

Determination activities

The evaluator performs a review of the documentation for the performance of audits by the cloud provider (e.g., TOM, procedure directories, procedure instructions, guidelines, role descriptions, audit and result protocols, scheduling of internal audits). In addition, the performance of an internal audit procedure can be ensured through representative sampling based on appropriate process documentation. Also, an evaluator can match the timing of (publicly known) changes to the cloud service (e.g., change and patch logs) with the timestamps of internal control procedure logs.

The practice of internal controls can be determined through interviews with the DPO and responsible persons during an audit. In particular, an evaluator will check whether staff members are aware of their assigned responsibilities according to the documentation and whether they carry out appropriate control procedures.

No. 8.6 – Selection and involvement of qualified persons (Art. 28 (3) subpara. 1 sent. 2 lit. e) and f) GDPR)

Criterion

(1) The cloud provider may entrust only employees, who are qualified to perform their respective tasks and are aware of and trained in data protection and data security, to carry out processing operations.

(2) The cloud provider must ensure that the employees have no conflicts of interest regarding the performance of their respective tasks.

(3) The cloud provider must ensure that employees are continuously trained in data protection and data security.

Explanation

It is a prerequisite to involve qualified employees for the cloud provider to be able to comply with its numerous duties in the first place. This criterion is also closely connected with criterion No. 8.1, as the DPO is responsible for the awareness and training of the employees involved in processing and carries out the respective reviews.

Implementation guidance

To maintain the specialised expertise of the employees, the cloud provider should conduct regular employee training workshops (roughly once a year) on data protection and information security issues, including the specific technology of the cloud service. The training of employees is a responsibility of the DPO.

Reference is made to the implementation guidance in BSI C5 HR-01, HR-02 and HR-03.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 7.1.2, 7.2.1, 7.2.2 and 7.3, and ISO/IEC 27701 no. 6.4.2.2, 6.8.2.9.

Determination methods

- Document review
- Auditing

Determination activities

An evaluator verifies the required expertise of staff through relevant evidence of qualification (e.g., template agreement, documentation on eligibility requirements for appointments, training documents, evidence of participation, role and authorisation concepts, process instructions, guidelines, role descriptions). Awareness-raising and training measures for employees can be verified by documenting training courses that have taken place.

The implementation of rules can be determined within the scope of an on-site audit (e.g., clean desk principle, screen locks) and interviews with employees (e.g., examination of expertise, awareness of guidelines, potential conflicts of interest).

Chapter IV: Data protection by system design

No. 9 – Data protection by design and by default

No. 9.1 – Data protection by system design (Art. 25 (1) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

(1) The cloud provider must conduct a risk analysis for all processing activities of its offered service and maintains TOMs within the scope of its offered service for the practical and expedient implementation of the data protection principles of Art. 5 GDPR (lawfulness, fairness and transparency, purpose specification, purpose limitation, data minimisation, accuracy, storage limitation, system data protection, and responsibility).

(2) The cloud provider must have processes in place for transparency and active monitoring of the state of the art at the levels of conceptual objectives, architecture, system design, and implementation.

(3) The cloud provider must ensure at all times that its system design in the offered applications and the service concept guarantee the traceability and transparency of the data processing, even when service chains are extended by potential sub-processor relationships.

Explanation

As the controller, the cloud user must fulfil the design obligations under Art. 25 (1) GDPR. As soon as the cloud user uses a cloud service, it must select a cloud provider that fulfils this obligation. The cloud service technology and organisation must therefore be designed in the way that is best to support the data protection principles of Art. 5 GDPR.

Implementation guidance

To meet the requirements of Art. 25 (1) GDPR, it is essential to take them into account in the modelling of data processing systems and processing operations at all levels. The principle of data protection by system design requires compliance with operational data protection requirements during the planning phase, so that non-data protection-compliant functions do not have to be implemented in the first place and subsequently deactivated. According to the SDM, the protection goals of the SDM can be interpreted as design principles or strategies for the design of the processing operations in compliance with data protection. Matured change management processes are required in order to react to changes in the legal framework and be able to use new, data protection-friendly techniques in existing processing systems. These include for example Privacy Enhancing Technologies (PETs) which can be used in the cloud service.

The measures to implement this criterion are very diverse. They range from the implementation of a data-minimised login for admission to the cloud service, roles and rights concepts for the administration of the processed data to erasure concepts for the erasure of this data. This also includes measures enabling the data subject to exercise his rights as data subject in the simplest way possible, as these rights increase transparency and control options for him. Examples of these measures are the requests for information according to Art. 15 (1) GDPR by clicking a button within the service or the online access to data that is stored about the data subject. The cloud provider should document the process of consideration that guided it in the selection of the TOMs to guarantee the data protection principles, as this selection requires that it considers the state of the art, implementation costs, likelihood and severity of the damage for the rights and freedoms of the data subjects with regard to the nature, scope, context and purposes of the processing.

Reference is made to the implementation guidance in ISO/IEC 29101 “Information technology - Security techniques - Privacy architecture framework”.

Reference is made to the implementation guidance in BSI C5 BEI-01 and BEI-02.

Reference is made to the implementation guidance in SDM D1.1 to D1.8.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.11, 8.4.

Reference is made to the implementation guidance in the EDPB’s Guidelines 4/2019 on Art. 25 GDPR.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

- Development and design review

Determination activities

To verify data protection by system design, an evaluator can use a variety of determination methods.

In the context of a document review, an evaluator checks the documentation of the cloud provider's data protection risk analysis. Using the processing directories, data flow diagrams or service descriptions of the service offered, an evaluator checks whether the risk analysis covers all processing activities of the cloud provider.

Through a document review, an evaluator also determines what design principles and measures a cloud provider has in place to minimise the identified risks and ensure compliance with the data protection principles. From the cloud provider's documents, the evaluator should also be able to understand what considerations guided the cloud provider in taking or not taking design measures so that the appropriateness of its evaluations and decisions can be assessed. Relevant documentation includes the risk analysis, service descriptions, the data security concept, role and authorisation concepts, process descriptions, process instructions, guidelines, the template contract for sub-processors, result protocols of internal audits and sub-processor controls, documentation of the information security management system, TOM, incident response management documentation and data protection impact assessments. The documentation in the mandatory processing directories according to Article 30 (2) of the GDPR and No. 8.3 of this catalogue can also serve as evidence for the system designs listed there. Protocols and other evidence of the implementation of organisational design processes can also be examined.

An evaluator should compare the documentation with the actual implementation of the measures through inspections, tests and (on-site) audits. For example, a trial service use (e.g., checking the functions and measures according to the service description), a process monitoring (e.g., to ensure encryption), and asset tests (e.g., source code analysis, analysis of system interfaces and hardware components) can be carried out in order to check whether the hardware or software used for data processing operations comply with the data protection principles. An interview or an observation of relevant staff should also be conducted to check their knowledge of policies and procedures and their competencies and responsibilities. The management board should also be interviewed to ensure that data protection through system design is embedded as a goal in the organisation and how decision-making processes and trade-offs are made.

In addition, a development and design review should be conducted to determine whether data protection requirements are already considered in the development of the system. For this purpose, evaluators can examine the development methods and procedures used (in particular, acceptance criteria and lists of requirements) on the basis of documentation and interviews with staff. An examination of test systems and environments (e.g., for adequacy and security) can be performed if required. During the design review, the selected architecture, database diagrams, data flow diagrams, design decisions, but also the configuration and default setting of the cloud service for the provision of the data processing operation can be reviewed.

An evaluator uses process documentation (e.g., logs of decisions, timestamps, versioning history, changelogs) and interviews with staff (e.g., awareness of policies and separation of responsibilities) to check how the state-of-the-art of technology is monitored and how changes to the state-of-the-art lead to adjustments of measures in the service offered.

Security tests can be used to support this, for example, to assess the security and appropriateness of design measures.

No. 9.2 – Data protection by default (Art. 25 (2) GDPR)

Criterion

(1) The cloud provider must ensure by default settings in the respective services that only personal data that are necessary for the relevant purpose of the processing are processed and personal data are only accessible to the extent necessary to fulfil the processing purpose of the cloud user.

(2) The cloud provider must ensure by default that personal data are not made accessible without the individual's intervention to an indefinite number of natural persons and that no risks arise for the data subject from providing access to personal data available in a too expansive extent.

Explanation

The controller must comply with the duties under Art. 25 (2) GDPR. As soon as it arranged for data processing being carried out on its behalf, the cloud user must select a cloud provider fulfilling this duty. The default settings of the cloud service must therefore be selected for fulfilment of the duty under Art. 25 (2) sent. 1 GDPR.

Implementation guidance

The measures to implement this criterion are very diverse. The cloud provider should use default settings to ensure that only personal data is processed that is necessary for the specific processing purpose. For this, not only the amount of processed data should be minimised, but also the extent of its processing, the storage period and accessibility of the data. If, for example, the use of the cloud service has to be logged to be able to detect misuse or ensure data security, the default setting should be selected so that the data is collected and processed anonymously.

Users can deviate from the privacy-friendly default settings, e.g., if they want more processing options. For this, good usability of the cloud service is just as important as information being given to the cloud user (e.g., in pop-up windows within the service) about the effects from changes being made to the default settings. Art. 25 (2) GDPR, however, requires that more extensive processing options are not preset, but that these can be switched on and activated by the cloud user as required. If the cloud provider has carried out a data protection impact assessment, requirements for the default settings can result from the obligation to minimise the identified risks.

Reference is made to the implementation guidance in ISO/IEC 29101 “Information technology - Security techniques - Privacy architecture framework”.

Reference is made to the implementation guidance in SDM D1.1 to D1.8.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.11, 8.4.

Reference is made to the implementation guidance in the EDPB’s Guidelines 4/2019 on Art. 25 GDPR.

Determination methods

- Document review
- Inspection
- Testing
- Auditing
- Development and design review

Determination activities

To verify data protection by default, an evaluator can use a variety of determination activities.

Through a document review, an evaluator determines which default settings a cloud provider has chosen and for what considerations. This should include a review of the documentation of the TOM, the data security concept, cloud service defaults, procedures, policies/concepts on passwords, authentication, access permissions, separation of test systems, and the documented development of the cloud service. Protocols and other evidence of the implementation of technical default settings or organisational design processes can also be examined.

An evaluator should compare the documentation with the actual implementation of the measures through inspections, tests and (on-site) audits. Among other things, a trial service use (e.g., checking the standard configuration to ensure that unnecessary processing operations are deactivated and preselecting data fields), operation monitoring (e.g., implementation of measures to separate development systems) and asset testing (e.g., source code analysis, analysis of system interfaces and hardware components) can be carried out to check default settings. An interview or an observation of relevant employees should also be carried out in order to check their knowledge of guidelines and procedural steps, their awareness of data protection, their data protection precautionary behaviour, as well as their competencies and responsibilities (in particular, with regard to the necessity of processing data). The management board should also be consulted to ensure that data protection by default is anchored as an objective in the company.

In addition, a development and design review should be conducted to determine whether the data protection requirements and default settings are already considered in the development of the system. For this purpose, evaluators can check the development methods and procedures used (in particular, acceptance criteria and selected default settings) on the basis of documentation and interviews with employees. A test of test systems and environments (e.g., for the implementation of default settings) can be performed if required. During the design review, data flow diagrams, design decisions, but also the configuration and setting of the cloud service for the provision of the data processing operation can be reviewed, among other things.

Security tests can also be used to assess e.g. the security and appropriateness of design measures.

Chapter V: Sub-processing

Explanation

For commissioned data processing on behalf of the controller, the principle of exclusively personal performance of the service possible applies. Under certain conditions, the cloud provider may engage other sub-processors. If a sub-processor hires further sub-processors, multi-level sub-processing relationships are established.

As the main processor, however, the cloud provider must ensure that the sub-processor also fulfils all obligations, which are to be fulfilled by the cloud provider as the main processor, unless it is exempted from this by law. Finally, the cloud provider continues to remain responsible to the cloud user for carrying out the processing.

No. 10 – Sub-processing relationships

No. 10.1 – Further processors of the cloud provider (sub-processing) (Art. 28 (2) GDPR)

Criterion

(1) The cloud provider must have a defined process, which ensures that a cloud service is provided with the involvement of sub-processors only if and insofar as the cloud user has given its prior specific or general authorisation for this sub-processing. The authorisation must be given in writing or in an electronic form. Approval is required only for sub-processes under which the further processor has the possibility to gain knowledge of processed personal data.

(2) If prior specific authorisation of sub-processing is given, the cloud provider must ensure that all sub-processors are designated by name and summons address and that the processing operations to be delegated to them are defined.

(3) The cloud provider must ensure that every sub-processor also guarantees all TOMs within the framework of its processing on behalf of the controller and complies with all obligations, which are also to be fulfilled by the cloud provider as the main processor, unless it is legally exempted from this. Every sub-processor must be able to demonstrate the same guarantees as the main processor.

Explanation

Not every service provider that is engaged is also a sub-processor. If the service provider does not process personal data, there is no subcontracted processing. This applies e.g., in the case that rooms are rented in a data centre (co-location), e.g., if access to data processing equipment and personal data is denied to the service provider based on TOMs. If sub-processes are placed, quality assurance and compliance with data protection in the service chain must be guaranteed by the cloud provider. In particular, the sub-processing may not complicate the protection of the rights of data subjects.

Implementation guidance

According to Art. 28 (2) sent. 1 GDPR, the involvement of sub-processors requires the authorisation from the cloud user. The authorisation can be granted specifically or generally. The specific authorisation is suitable for those cases in which it is foreseeable that sub-processors will only be used in exceptional cases and no changes are expected. The general authorisation should be used if it is already clear at the time of the conclusion of the legally binding commissioned data processing agreement that numerous sub-processors are to be involved and if the cloud provider agrees to this.

For standardised bulk transactions, cloud users can be informed automatically of changes in sub-processing, e.g., via an automatically generated email. A general agreement in advance into any changes in sub-processing, which are subject to reservations, can also be obtained, e.g., the general terms and conditions of cloud providers for bulk transactions. Since an objection (within the meaning of Art. 28 (2) sent. 2 half-sentence 2 GDPR) by an individual cloud user will not prevent the cloud provider from commissioning an additional or another processor when it comes to bulk transactions, the legally binding commissioned data processing agreement (no. 1.7) should determine the requirements and consequences of an objection, e.g., whether the cloud user may terminate the agreement in the event of an objection.

Reference is made to the implementation guidance in BSI C5 DLL-01 und DLL-02.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 15, ISO/IEC 27018 no. A10.12 and ISO/IEC 27701 no. 6.12, 8.5.6 and 8.5.7.

Determination methods

- Document review, particularly legal analysis

- Auditing

Determination activities

An evaluator performs a document review by verifying the consents given by the cloud users. In the case of standardised cloud services, the standardised legally binding agreements and any general consents contained therein must be checked. In the case of individual agreements with cloud users, these must be checked on a sample basis, and existing agreement templates must be checked. If further documentation of the consent is available, these must be checked on a sample basis. Finally, it can be checked whether a change to the agreement templates or general consents was carried out after a new agreement was concluded with a sub-processor (e.g., timestamp, versioning, changelog).

In the course of an audit, the evaluator can also interview the responsible staff members to check whether the established process for involving and changing sub-processors is known and practised. The determination activities regarding the obligations of the sub-processor(s) are carried out in the following criteria.

No. 10.2 – Legally binding agreement as the basis for sub-processing (Art. 28 (4) GDPR)

Criterion

(1) The cloud provider must ensure that its sub-processors act exclusively on the basis of a legally binding sub-processing agreement that is in accordance with the legally binding commissioned data processing agreement between the cloud provider and cloud user.

(2) The cloud provider makes its sub-processors subject to the obligation of ensuring that their subcontracted processors also act on the basis of a legally binding sub-processing agreement and transfer the same obligation to their sub-sub-processors.

Implementation guidance

Reference is made to the implementation guidance in ISO/IEC 27002 no. 15.1.2, 15.1.3, ISO/IEC 27018 no. A10.12 and ISO/IEC 27701 no. 6.12, 8.5.6 and 8.5.7.

Determination methods

- Document review, particularly legal analysis

Determination activities

The evaluator should inspect the list of sub-processors used and carry out a sample check of agreements concluded with sub-processors. An evaluator checks the agreements with the sub-processors to assess completeness and admissibility of the contents according to Art. 28 (3) and (4) GDPR (check for, among other things, duration, type and purpose, place of further processing, information on the processor and its service description, information on further involved sub-processors and their service description as well as the obligation to comply). For the respective sub-processors, existing documents of the TOM, the data security concept or certificates should be checked on a sample basis. Further relevant documents can be included in the review, including the template contract for processing with sub-processors, guidelines and instructions, further guarantees of the sub-processors, internal control departments of the cloud provider on sub-processor controls, the data protection concept or the risk assessment for subcontracting.

No. 10.3 – Informing the cloud user (Art. 28 (2) sent. 2 GDPR)

Criterion

(1) If general authorisation is given, the cloud provider must inform the cloud user about the identity of all sub-processors it involves at all levels (including their summons addresses) and about the processing that should be carried out by them.

(2) The cloud provider must always inform the cloud user about any intended changes relating to the involvement or replacement of other sub-processors and must guarantee that the cloud user can exercise its right to object at all levels of the commissioned data processing.

Explanation

Even if a general authorisation of sub-processors is given, the cloud user must be able at all times to find out which sub-processors are involved in which processing step, and what data processing is carried out by which sub-processor and at what processing level, which is why the cloud provider has a duty to provide information.

Implementation guidance

As the main processor, the cloud provider should draft detailed documentation of the involved sub-processors for each extension of the commissioned data processing service chain, disclosing their identity including their summons address and the carried out activities to make clear which (sub-) processor is involved, respectively, in the parts of the service that are critical for data protection and which processing operations are carried out by whom. This requires that the sub-processor inform the cloud provider about the sub-processors engaged by it and provide the necessary information (cascading provision of information).

Information platforms within or outside the offered cloud service are suitable for showing which sub-processors are involved. They should be maintained and updated on a continuous basis.

Reference is made to the implementation guidance in ISO/IEC 27018 no. A7.1 and ISO/IEC 27701 no. 8.5.2, 8.5.6 and 8.5.8.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

An evaluator examines the documents describing how a cloud provider provides information about involved sub-processors to cloud users (e.g., in the legally binding agreements, in the form of general consents, in information portals) and how the provider informs them of intended changes to sub-processors and receives and processes objections from cloud users. In addition, the evaluator checks the documentation on the sub-processors involved for completeness (e.g., the identity, address, and the processing carried out). The evaluator may also review other relevant documents, such as template agreements with cloud users, documentation of cloud users' consent and exercise of the right to object, and other policies. The evaluator can inspect the list of subcontractors used, carry out sample checks of cloud user agreements concluded, and check the availability of the information for the cloud user. Finally, it is possible to check whether a change to the agreement templates or general agreements with cloud users has been made after a new agreement has been concluded with a subcontractor (e.g., timestamp, versioning, changelog). Logs of notified changes to sub-processor involvement or processed user objections should be reviewed by the evaluator, if available.

An inspection in the form of process monitoring or an observation in the context of an audit can be used to check whether all necessary information on the involvement of sub-processors is communicated to the cloud user in an appropriate manner. For this purpose, a request from a cloud user can be simulated by an evaluator as a test. Similarly, the processing of an objection by a cloud user can be checked. An interview of relevant employees can be conducted (e.g., to assess their knowledge of policies, receiving requests and objections from the cloud user, etc.).

No. 10.4 – Selection and control of the sub-processors (Art. 28 (4) sent. 1 GDPR)

Criterion

(1) The cloud provider must ensure that at all levels, sub-processors are only involved if they offer a guarantee of compliance with the legal data protection requirements for the service they are providing.

(2) The cloud provider must satisfy itself of all hired sub-processors fulfilling the legal data protection requirements for the services they are providing.

Implementation guidance

Insofar as the cloud provider cannot rely on the certificates of its sub-processors, it should satisfy itself that the sub-processors comply with the legal data protection requirements.

Reference is made to the implementation guidance in BSI C5 DLL-01 and DLL-02.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 15.2.1, ISO/IEC 27018 no. A10.12 and ISO/IEC 27701 no. 8.5.6.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

An evaluator examines existing documents of the sub-processors used (code of conducts, certificates, legally binding agreements, service descriptions, data security concepts, other guarantees), which provide assurance of compliance with the GDPR. In addition, the evaluator shall examine documents on the selection (e.g., records of selection considerations and decisions) and the performance of cloud provider's own checks (e.g., records of subcontracted processor checks).

In the sense of an inspection, a commissioning and control of a sub-processor can be simulated, in which an evaluator checks whether the procedural steps are carried out completely and correctly. Different test sub-processors can be selected, for example, a company that does not meet the data protection requirements, so that the selection process should reveal this problem. In the course of this, competencies of the employees and correct competencies and responsibilities can also be checked.

These assessments can be supported by interviews with employees about performing controls of sub-processors (e.g., awareness of procedural steps and guarantees of subcontractors). It can also be checked whether individual departments have commissioned or use further sub-processors, which were not previously known to the evaluator.

No. 10.5 – Ensuring the support functions
(Art. 28 (4) sent.1 in connection with Art. 28 (3) subpara. 1 sent. 2 GDPR)

Criterion

(1) The cloud provider must ensure that even when (several) sub-processors are engaged, its support functions besides its obligations as the main processor are fulfilled to the extent agreed.

(2) The cloud provider must ensure, by means of appropriate processes and precautions that the extension of the service chain in the processing will not lead to less compliance with the legal data protection standards and obligations.

Implementation guidance

The cloud provider should maintain internal documentation and log the processing in light of the increased risk associated with further sub-processing. This also serves as the self-control of the cloud provider for the fulfilment of obligations on the further contracting levels. Depending on the outsourced processing activities in question, the relevant support functions should be documented in the legally binding agreement with the sub-processor. In particular, points of contact and the respective responsibilities for sub-processors should be logged and continuously updated. Processes, reporting channels and procedural guidelines should be defined and documented.

Reference is made to the implementation guidance in ISO/IEC 27002 no. 15.1.3, ISO/IEC 27018 no. A10.12 and ISO/IEC 27701 no. 8.5.

Determination methods

- Document review
- Auditing

Determination activities

An evaluator examines documents submitted on the cloud provider's procedures and arrangements for engaging sub-processors, including legally binding agreements with sub-processors, process documentation on involvement, data security concepts and information on contact persons for sub-processors, risk analyses or documents on the separation of responsibilities for individual processing operations. Protocols for the fulfilment of obligations in case of the involvement of additional processors should be examined.

An audit can be supported by interviews of employees on the involvement of sub-processors to support the cloud provider on its duties as the main processor (e.g., awareness of procedural steps and contact persons of the sub-processors).

Chapter VI: Processing outside of the EU and EEA

No. 11 – Data transfers

No. 11.1 – Appropriate safeguards for data transfers; measures for protection against disclosure of data to public authorities of third countries (Art. 45, 46 and Art. 48 GDPR)

Criterion

(1) The cloud provider may transfer personal data to third countries or international organisations if it has verified that there is a decision by the European Commission in accordance with Art. 45 (3) GDPR for the recipient state or international organisation, stating that an adequate level of protection applies there and if the cloud provider regularly assesses whether the adequacy decision continues to apply.

(2) Alternatively, the data transfer may take place if the cloud provider, after assessing law and practice of the third country, ensures that the appropriate safeguards within the meaning of Art. 46 (2) or (3) GDPR, set out in the legally binding commissioned data processing agreement, are used and that they ensure an adequate level of protection that is equivalent to that of the General Data Protection Regulation.

(3) If, after assessing law and practice of the third country, the appropriate safeguards within the meaning of Art. 46 (2) or 3 GDPR as specified under the legally binding commissioned data processing agreement prove to be insufficient for ensuring an adequate level of protection equivalent to that of the General Data Protection Regulation, the cloud provider must take supplementary measures to ensure this adequate level of data protection. Otherwise, the data transfer may not take place.

(4) The cloud provider must continuously monitor the adequacy of the level of data protection and ensure by means of TOMs that data transfers are immediately suspended or terminated if, in the case of para. 2 or 3, the recipient has infringed the obligations it has entered into under the appropriate safeguards of Art. 46 para. 2 or 3 GDPR or its fulfilment is impossible and in the case of para. 3 the supplementary measures can no longer be complied with or are ineffective.

(5) Cloud providers, who process personal data and are subject not only to the law of the General Data Protection Regulation, but also to the law of a third country, which obliges them to disclose this personal data to public authorities of the third country, must take supplementary measures to effectively protect personal data from being disclosed to public authorities of the third country. The cloud provider must ensure that personal data is only disclosed to public authorities of third countries if the disclosure is based on an international agreement in force between the requesting third country and the EU or Germany.

Explanation

Transfers of personal data of data subjects to third countries are only permitted under the conditions set out in Art. 44 et seq. GDPR. The same applies to the transfer of personal data to an international organisation for which no adequate level of data protection is recognised.

If the commissioned data processing includes the instruction for a data transfer to third countries or international organisations, Art. 44 GDPR also requires compliance with the requirements of Chapter 5 GDPR. It should be noted that the regulation of Art. 49 GDPR does not contain any permissions for the systematic and regular data transfer between exporter and importer, as it is customary in cloud computing. Systematic and regular data transfers between exporter and importer must therefore be based on adequacy decisions pursuant to Art. 45 (3) GDPR or the appropriate safeguards pursuant to Art. 46 (2) or (3) GDPR, which have been determined between the cloud provider and the cloud user in accordance with no. 1.4. Data transfers on the basis of Art. 49 GDPR may take place, if at all, only in very restrictive exceptional cases which, however, are not covered by this Criteria Catalogue.

Art. 46 (2) and (3) GDPR names various transfer instruments, which can be appropriate safeguards to ensure an adequate level of protection in the third country and be applied uniformly to all third countries. Due to the special legal and/or practical circumstances in a third country to which personal data is to be transferred, it may be necessary, however, for the cloud provider to supplement these transfer instruments with supplementary organisational, technical and / or contractual measures to ensure an adequate level of data protection, which essentially corresponds to that of the General Data Protection Regulation.

It is to be noted that the use of the EU standard contract clauses of June 2021 (EU SCC) alone does not ensure an adequate level of data protection. Rather, the cloud provider, if necessary, together with the recipient, must also assess for this transfer instrument, whether law and practice of the third country impair the effectiveness of the EU SCC. This assessment must also be carried out when using the other appropriate safeguards according to Art. 46 (2) and (3) GDPR. If there is an impairment, the data transfer must not take place or supplementary measures must be taken to close the identified gaps and ensure an adequate level of data protection in the third country.

Cloud providers may be subject to the law of a third country, which obliges them to disclose personal data to public authorities of the respective third country, if they process data in whole or in part in the respective third country, but also if they, e.g. as a European subsidiary of a parent company domiciled in a third country, process personal data exclusively on servers in the EU or in the EEA. In this case, the cloud provider may also be obligated under the law of third countries to disclose personal data kept on servers in the EU or in the EEA to public authorities of the third country in question if it is ordered to do so by judgement of a court or tribunal decisions of administrative authorities. This is the case, e.g. for European subsidiaries of US parent companies under the US CLOUD Act. Such legal disclosure obligations under the law of third countries conflict with Art. 48 GDPR. This norm obligates controllers and processors to comply with any judgements of courts or tribunals of third countries and any decisions by administrative authorities of third countries that require the disclosure of personal data, only if they are based on an international agreement in force such as a Mutual Legal Assistance Treaty between the requesting third country and the Union or a Member State.

Implementation guidance

Reference is made to the implementation guidance in ISO/IEC 27018 no. A11.1 and ISO/IEC 27701 no. 6.15, 8.5.

In its "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", the European Data Protection Board published a six-step roadmap that specifies how the cloud provider should proceed in order to determine whether the instruments according to Art 46 (2) or 3 GDPR are sufficient to ensure an adequate level of data protection for the transfer of data to the third country in question, or if supplementary measures must be taken to ensure an adequate level of data protection. Reference is therefore made in particular to this six-step roadmap in the Recommendations 01/2020 as implementation guidance.

Special attention should be paid to the steps 3 and 4 of the roadmap. In step 3 of the roadmap, it is to be assessed whether law and practice of the third country impair the effectiveness of the appropriate safeguards according to Art. 46 (2) or (3) GDPR in the specific data transfer and, if this is the case, it should be assessed in the step 4 of the roadmap whether supplementary measures can be effectively taken to ensure an adequate level of protection. Firstly, as part of the examination of the third step, the legal provisions of the third country concerned should be examined.

The following legal provisions, which implicitly or explicitly regulate legal powers of public authorities to access personal data, can be taken into account for the assessment of law and practice in the following countries, whereby this list is exemplary and not exhaustive in relation to the countries and the legal provisions[4]:

1. USA: Foreign Intelligence Surveillance Act (FISA), Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Executive Order 12333 (United States intelligence activities)

   Cloud providers based in the USA are subject to the US FISA that grants permission to the US public authorities in Sec. 702 FISA to access data of non-US citizens, which are processed by US companies ("electronic communication service providers") and stored in the USA. For this legal norm, the ECJ established that the access rights to personal data are not limited to what is necessary and proportionate in a democratic society, so that the use of appropriate safeguards according to Art. 46 (2) or (3) GDPR for data transfers alone does not lead to an equivalent level of data protection in the USA.

   The CLOUD Act also enables US public authorities to force US companies to grant access to data of non-US citizens if the companies are able to provide this access, even if these data are kept on European servers. This applies in the case of a cloud provider that is a European subsidiary of a US parent company. These access rights go beyond what is necessary and proportionate in a democratic society. After all, in the case of personal data of Europeans, the company that is subject to the CLOUD Act hardly has any effective means of having the order of the US public authority reviewed by a court, as this possibility only exists if the disclosure would induce the recipient to violate the laws of qualified foreign governments. Neither Germany nor the EU has signed an executive agreement with the US that would make them such a qualified foreign government. An independent oversight mechanism as one pillar of the European Essential Guarantees is consequently not present, so that no equivalent level of data protection can be assumed. Furthermore, such disclosure contradicts Art. 48 GDPR, as there is no Mutual Legal Assistance Treaty between Germany/the EU and the USA, and as personal data may therefore not be passed on to the US public authorities.

   Executive Order 12333 aims to provide intelligence to the President, the National Security Council and the Homeland Security Council. An effective limitation of the measures for the gathering of information to US citizens only is not provided in the Executive Order, which also prevents an equivalent level of protection.

2. Russia: Federal Law on "Foreign Reconnaissance" of 10.1.1996 No. 5-FZ (Федеральный закон от 10.1.1996 г. N 5-ФЗ "О внешней разведке"), Federal Law on "the Federal Security Service" of 3.4.1995 (Федеральный закон "о федеральной службе безопасност" от 03.04.1995 г. N 40-ФЗ), Federal Law "on operational search activities" of 08.12.1995 No. 144-FZ (Федеральный закон "Об оперативно-розыскной деятельности" от 08.12.1995 г. N 144-ФЗ), Federal Law "on Communication" of 7.7.2003 No. 126-FZ

[4] The selected examples correspond to the legal status of September 2021 and will not be updated.

(Федеральный закон "О связи" от 7.7.2003 г. N 126-ФЗ). These regulations permit public authorities to use companies from Russia for intelligence purposes and to force them to disclose personal data.

3. China: National Intelligence Law of the People's Republic of China of 27.6.2017, Cryptography Law of the People's Republic of China of 26.10.2019, Counterterrorism Law of the People's Republic of China (Order No. 36) of 27.12.2015. These regulations permit public authorities to use companies from China for intelligence purposes and to force them to disclose personal data.

However, legal regulations should not be used as the only source of information, as they can formally suggest an equivalent level of data protection, which is meanwhile not guaranteed in the legal practice. In addition to the legal regulations themselves, the following sources of information should therefore also be taken into account if available for the third country in question:

- The case law of the ECJ such as the Schrems II judgment for the USA or the case law of the European Court of Human Rights (ECHR) such as the factsheet on mass surveillance;
- Adequacy decisions for the third country if the data transfer relies on a different transfer instrument;
- Resolutions and reports of intergovernmental organisations such as the Council of Europe or regional bodies, e.g. the country reports of the Inter-American Commission on Human Rights or United Nations organisations like the Human Rights Council or the Human Rights Committee of the United Nations;
- Reports and analyses of competent regulatory networks such as the Global Privacy Assembly (GPA);
- National case law or decisions taken by independent judicial or administrative authorities competent on data protection and the protection of privacy of third countries;
- Reports of independent oversight or parliamentary bodies;
- Reports based on practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, from entities active in the same sector as the recipient;
- Warrant canaries[5] of other entities processing data in the same sector as the recipient;
- Reports produced or commissioned by Chambers of commerce, business, professional and trade associations, governmental diplomatic, trade and investment agencies of the exporter or other third countries exporting to the third country to which the transfer is made;
- Reports from academic institutions, and civil society organizations (e.g. NGOs).

The recipient's practical experience may be incorporated into the overall assessment of the third country's level of protection, but it must not rely exclusively on this. If possible, practical experience should be backed up, e.g. by experience reports from other companies operating in the same sector or, e.g. by investigative articles published by reputable newspapers or academic essays published in professional journals, which discuss the specific law and actual practice. If the recipient has not received any disclosure requests so far, this should not lead to conclude that none could be expected in the future either. All sources of information that are used to assess law and practice must be carefully documented. Legal regulations are to be documented citing the full title of the legal provision and the relevant sections. Reports, judgments, etc. included in the assessment must also be clearly identified. In this respect, it is advisable to keep the source of information management up to date.

When assessing law and practice of the third country, it is important to check whether the specific data transfer falls within the scope of laws that grant public authorities in the third country the power to access personal data that go beyond what is a necessary and proportionate measure in a democratic society. For this assessment, the "European Essential Guarantees" of the "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures" can be used as a standard of reference.

The following statements on the European Essential Guarantees is a shortened summary of the "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures", providing initial guidance for the cloud provider in the assessment of law and practice of third countries. The four European Essential Guarantees should be seen as core elements, which should not be assessed independently but rather in their entirety, when assessing whether or not measures to access personal data by public authorities of third countries are limited to what necessary and appropriate in a democratic society. For further information on the assessment, reference is made to the recommendations 2/2020.

[5] These are cryptographically signed messages sent at regular intervals, which inform the data exporter that the data recipient has not received a request for disclosing personal data or similar up to a certain point in time (date and time). If such a message is not sent, this indicates to the data exporter that the data recipient could have received such a request.

The four European Essential Guarantees are:

1. **Clear, precise and accessible rules for data processing**

   Legal provisions governing access to personal data by public authorities must provide clear, precise and publicly accessible rules for the application of the access measures in question and impose minimum safeguards for them. This also means that the legal regulation has to define the circumstances and conditions under which an access measure may be used by the public authority, and the extent to which the rights to privacy and the protection of personal data of the data subject may be limited. In addition, the legal regulation must define the following: categories of people, who may be affected by access measures, limits on the duration of the access measures, the procedure to be followed for examining, using, and storing the data obtained, and the precautions to be taken for the transfer of the data to other parties. Furthermore, the legal regulation must be binding and grant data subjects rights against the public authority, which they can assert and enforce in court. If there are no publicly accessible regulations that govern access to personal data by public authorities or if the data subjects are not granted any rights against the authority, no equivalent level of protection can be assumed for the third country.

2. **Proof of necessity and proportionality with regard to the legitimate objectives pursued**

   In accordance with Art. 52 (1) sent. 1 CFR (Charter of Fundamental Rights of the European Union), any limitation of the rights recognised by the Charter must respect the essence of these rights, which is why limitations through access measures may only be made if they are necessary while maintaining the principle of proportionality and if they genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The assessment of whether a limitation is proportionate depends, on the one hand, on the severity of the interference entailed by a limitation and, on the other hand, whether the public interest objective pursued by the limitation is proportionate to the severity of the interference. For example, access by public authorities to the location of a data subject's mobile phone in real time is a serious interference because it enables the public authority to track the movements of the data subject at any time. However, it could be proportionate if it aims, e.g. at preventing imminent, serious acts of terrorism or searching for injured or missing persons. The limitation of a right must be limited to what is strictly necessary, which presupposes that for the access measures it must be precisely regulated by legal provisions when, under which circumstances and conditions the access measures may be used and what minimum safeguards must be observed by the public authority. Legal provisions that allow interferences within the meaning of access measures to personal data by public authorities without providing limitations, do not meet the requirements for an equivalent level of data protection, since every legal provision for an interference must define the scope of the limitation of the respective rights. Furthermore, the principle of necessity is not complied with if legal provisions for access measures disrespect the essence of rights. This is the case, e.g. regarding Art. 7 of the Charter if public authorities are permitted under legal provisions to generally access the content of electronic communication without the interference being limited, the objectives pursued by the interference being named and objective criteria for the use of the access measure being defined.

3. **Independent oversight mechanism**

   Furthermore, an effective, independent and impartial oversight mechanism by a judge or another independent body must be provided in the third country for any interference with the rights to privacy and data protection. On the one hand, the oversight mechanism must ensure that some access measures by public authorities are made dependent on the prior approval by a judge or an independent body, and that this approval or rejection is binding. On the other hand, the oversight mechanism must have all the powers to be able to carry out controls effectively and identify abusive actions by public authorities. This requires, e.g. access to all relevant documents including classified information. The independence of the oversight mechanism also requires it has sufficient independence from the executive. It is just as important, however, that the activity of the oversight body itself is subject to public control, i.e. its conclusion can also be verified independently and impartially.

4. **Effective remedies**

   According to Art. 47 (1) of the Charter, every person, who considers that his rights and freedoms guaranteed by the law of the European Union are violated, has the right to an effective remedy before a court. This requires, e.g. in the case of interferences with the rights to privacy and the protection of personal data, which take place in secret, a subsequent notification of the data subject. An equivalent guarantee must also be given in the third country, which means that the data subject in the third country must have the opportunity to seek remedy before an independent and impartial court or body to obtain access to the personal data concerning him or its rectification or erasure. In particular, the court or body must be independent from the executive and be empowered to make binding decisions against the relevant public authorities.

If the assessment of law and practice in the third country leads to the result that the instruments of Art. 46 (2) and (3) GDPR are not sufficient to ensure an adequate level of data protection, the data transfer must not take place without supplementary measures.

If the data transfer should take place anyway, the cloud provider, if necessary, together with the recipient, should check in step 4 of the roadmap whether supplementary measures can ensure an adequate level of protection in the third country. In principle, supplementary measures can be of a contractual, organisational or technical nature. In order to achieve an equivalent level of protection in the third country, a combination of several measures can be useful.

For example, a contractual assurance by the recipient that it has not intentionally included back doors, other technical possibilities or business processes that provide public authorities with or facilitate access to the cloud service and personal data and pursuant to the national law of the third country, he is not obligated to include back doors in the cloud service, grant public authorities access to the cloud service or personal data nor own or surrender encryption keys. It is also sensible to obligate the recipient to inform the exporter immediately if changes in national law or legal practice entail that the given assurances can no longer be met, so that the exporter can terminate the contract at short notice and end the data transfer. It should be noted, however, that such assurances by the recipient might be prohibited under the national law of the third country.

If a recipient is subject to national laws such as FISA, CLOUD Act or similar laws of other third countries, contractual and organisational measures alone will usually not be sufficient to prevent access to personal data by public authorities of the third country, so that technical measures should be taken.

The following three use cases are intended to provide assistance as to when additional technical measures can contribute to an equivalent level of protection and when not:

1. Use case: data storage in the cloud service, e.g. for backup purposes, where the recipient does not require access to personal data in the clear. The encryption before the data transfer is an effective additional technical measure if

    a. Strong encryption is chosen and the identity of the recipient is verified;

    b. The encryption algorithm and its parameterization (e.g. key length, operating mode) conform to the state-of-the-art and - taking into account the available resources and technical capabilities (e.g. computing power for brute force attacks) – offer robustness against the cryptanalysis performed by the public authorities in the third country;

    c. The strength of the encryption takes into account the time period for which the confidentiality of the encrypted personal data must be preserved;

    d. The encryption algorithm is implemented without errors by properly maintained software, whose conformity with the specification of the algorithm chosen has been verified;

    e. The keys are reliably managed by the exporter (generated, administered, stored, if relevant, linked to the identity of the intended recipient and revoked); and

    f. The control over the keys is retained solely with the exporter or with other bodies entrusted with this task in the EEA or in a third country with an adequacy decision.

    The requirements KRY-01, KRY-03 and KRY-04 of the BSI C5 contain guidelines for the use of encryption procedures and for secure key management, which should be followed in the implementation of the applied encryption. ISO/IEC 11770-2 also contains further information on key the management of keys. Furthermore, the technical reports of the BSI TR-02102-1 "Cryptographic mechanisms: Recommendations and Key Lengths"; BSI TR-02102-3 "Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)"; and BSI TR-02102-4 “Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Secure Shell (SSH)” offer further helpful information on encryption, which is why reference is made to them.

    The current version of the “Guideline: State of the Art” by TeleTrust can also be referred to for the state of the art in encryption procedures and other TOMs.

2. Use case: processing of pseudonymised data by the recipient. The pseudonymisation of the data by the exporter before the data are transferred to the recipient is an effective supplementary technical measure if

    a. An exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group without the use of additional information,

b. That additional information is held exclusively by the exporter and kept separately in a Member State or in a third country, by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA,

c. Disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, and it is ensured that the exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and

d. The controller has established by means of a thorough analysis of the data in question - taking into account any information that the public authorities of the recipient country may be expected to have - that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.

Furthermore, the explanations in paragraphs (i.e. margin numbers) 86 to 89 of recommendations 01/2020 should be noted.

Information regarding the legally compliant implementation of pseudonymisation procedures can be found in the working paper "Requirements for the use of pseudonymisation solutions in compliance with data protection regulations" by Schwartmann/Weiß, to which reference is made.

3. Use case: Data transfer to a cloud service that requires access to unencrypted data due to the type of commissioned data processing. If the law of a third country applies to the recipient, which grants public authorities access to personal data that goes beyond what is necessary and proportionate in a democratic society, technical measures such as transport encryption during transfer and the encryption of personal data at rest is not sufficient to protect the rights of the data subjects. The combination of the named technical measures with supplementary contractual measures such as the contractually guaranteed obligation of the importer to challenge the requests of disclosure received from public authorities and to pursue legal recourse in the national courts against a disclosure request or the contractual obligation to inform the exporter of any disclosure requests received before the data are transferred to the public authority is not sufficient to legitimate a data transfer to the third country in question. In use case 3, no data transfer should therefore take place.

A non-exhaustive list of conceivable supplementary contractual, organisational or technical measures, as well as a list of further use cases is contained in Annex 2 of the Recommendations 01/2020 to which reference is made.

According to Art. 48 GDPR, cloud providers, who are also subject to the law of third countries, must reject requests for the surrender of personal data from public authorities of third countries with regard to personal data from the EU and the EEA, and refer to international agreements in force, such as legal assistance treaties, insofar as these exist with the third country concerned.

If the cloud provider processes personal data and is not only subject to the law of the General Data Protection Regulation but also to the law of a third country, which obligates it to disclose this personal data to public authorities of the third country concerned, supplementary measures are to be taken for the protection of the European fundamental rights and freedoms of the data subjects so as to protect the personal data from being disclosed to public authorities of the third country. One possible solution is, e.g. a trust model in which the data remains in the possession and control of a company that is exclusively subject to European law. For this, reference is made to the explanation in criterion no. 1.5. With regard to other conceivable supplementary measures that must be taken to protect European fundamental rights and freedoms, the supplementary measures under Annex 2 of the Recommendations 01/2020 of the European Data Protection Board may also be helpful in some cases, which is why reference is made to it. In this case, too, it should be noted that supplementary contractual or organisational measures will usually not be sufficient to protect personal data from disclosure to public authorities of third countries, so that they should be combined with technical measures.

Determination methods

- Document review, particularly legal analysis
- Inspection
- Testing
- Auditing

Determination activities

An evaluator performs a document review. In doing so, the evaluator checks the list of sub-processors used in third countries or the list of countries to which data is transferred, as well as other documents (e.g., a contract template for the recipient obligation). An evaluator checks whether a decision of the European Commission pursuant to Article 45 (3) of the GDPR exists for the recipient state or the international organisation or whether the cloud provider can provide documents on the agreed appropriate safeguards according to Article 46 (2) or (3) of the GDPR or existing certifications pursuant to Article 42 (2) of the GDPR and the supplementary legally binding and enforceable

obligations to apply the appropriate safeguards. If the third country transfer is based on agreed appropriate safeguards pursuant to Article 46 (2) or (3) of the GDPR, the cloud provider's documentation on the assessment of the legal situation and legal practice in the context of the six-step roadmap of the European Data Protection Board in the third country in question must be reviewed as part of a document review. An evaluator should review the documentation for all six steps of the roadmap. The evaluator checks whether the sources included in the assessment, such as legislation, the case-law of the ECJ or national courts, reports of intergovernmental organisations, reports on experiences of legal practice, etc., are sufficient to assess compliance with the essential European safeguards and thus the adequacy of the level of data protection in the third country for the specific data transfers. For this purpose, the evaluator should obtain the cloud provider's specific explanations on compliance with the essential European guarantees in the respective third country. Where the evaluator, based on his certification experience for the cloud service, is aware of relevant, from a European perspective, problematic regulations of the third country regarding the access of state authorities to personal data, the evaluator additionally checks whether these regulations are also listed and dealt with in the documentation of the cloud provider. Interviews with the employees involved in the assessment of the level of data protection can also be carried out (e.g., knowledge of the procedural steps for the assessment of the adequate level of protection and the relevant sources that should be included in the assessment, knowledge of the essential European guarantees and how their compliance or non-compliance is to be checked).

If the cloud provider's explanations lead to the conclusion that the legal situation and legal practice in the third country do not meet the essential European safeguards, the evaluator examines the cloud provider's documentation on the additional measures taken after step 4 of the roadmap to ensure an adequate level of data protection in the third country as part of a document review. In particular, an evaluator should assess whether the additional measures are sufficient to address the gaps in protection that exist in the third country and lead to an inadequate level of data protection.

The methods of determination used by the evaluator will depend on the nature of the additional measures: For example, if the cloud provider contractually promises not to have backdoors or similar technical measures built into the cloud service that provide or facilitate access to the cloud service and the personal data by third-country governmental authorities, the evaluator will examine the relevant clauses in the contract as part of a document review. In addition, the cloud service should be checked on a sample basis by the evaluator for suspicious data outflows in the course of an inspection.

Agreed organisational measures should be checked in the context of a document review by submitting, for example, transparency reports received or "warrant canary" declarations of the recipient.

The evaluator may also review further documentation on measures taken by the cloud provider to regularly check the adequacy of the level of data protection in the third country, for example, proactive queries to recipients about changes in the law in the third country concerned, processing of regular notifications made by the recipient to the cloud provider on the basis of contractual obligations regarding changes in the law or requests from government bodies. Furthermore, documentation on measures, procedures and responsibilities taken by the cloud provider should be reviewed if the level of data protection in the third country is no longer adequate and the data transfer is therefore discontinued. An interview can also be carried out here as part of an audit with the responsible employees, for example, to assess their knowledge of the relevant procedure in this case.

The presentation of a currently valid certification according to Article 42 (2) of the GDPR, which has already been obtained for data processing operations of the certification object to be certified, can also be checked by an evaluator. In this case, the evaluator's review also extends to the binding nature and enforceability of the commitment to apply the appropriate safeguards.

If encryption is used, the documentation for the respective procedure should first be checked as part of a document review. On the basis of the current technical requirements and guidelines, for instance from the BSI, the evaluator should check whether strong encryption has been selected, which also takes into account the period of time for which the confidentiality of the encrypted data is to be ensured, the encryption algorithm corresponds to the state-of-the-art with regard to its key length and other parameterisation, and how the key management is organised. For this purpose, the evaluator can inspect documentation on the encryption procedure, guidelines, protocol and log data, result protocols of internal/external audits and risk analyses.

The implementation of the encryption process is determined and checked for adequacy during an inspection and/or test through representative sampling. It should also be checked how keys are generated, and key management is structured and whether the keys are held solely by the exporter or by other bodies entrusted with this task in the EEA or, in a third country, with an adequacy decision. The software for encryption and its configuration should also be examined as part of an asset test and checked for the presence of anomalies. Likewise, the correct storage of the encrypted data is determined by a test. The implementation and security of the encryption procedures are determined by representative technical tests (e.g., penetration tests) and checked for adequacy.

If pseudonymisation is used, the documentation for the respective procedure should first be checked as part of a document review. The evaluator checks how the pseudonymisation is carried out so that it is no longer possible to refer to a person without the additional information and how the identification files are stored and protected at the

exporter. For this purpose, documentation of the TOM, guidelines, protocol and log data, result protocols of internal/external audits or risk analyses can be examined, among others. An interview of employees should also be conducted to check whether they are aware of and implement the current recommendations on pseudonymisation.

The implementation of the pseudonymisation procedure should additionally be determined and checked for adequacy within the scope of an inspection and/or test by representative samples. Likewise, the correct processing of the pseudonymous data is determined by a test. To this end, the type of programs used, the programming for pseudonymisation and their configuration should be checked as part of an asset test, and a random check of data records should be carried out.

A review of the effectiveness of the TOM taken to protect the additional identifiability information is also required to establish that control over the pseudonymisation algorithm or the data store that enables re-identification using the additional information is vested solely in the exporter, exclusively in a Member State or in a third country with an entity in the EEA entrusted by the exporter or in a jurisdiction offering a level of protection substantially equivalent to the EEA, and therefore neither the pseudonymisation algorithm nor the data store enabling re-identification from the additional information is subject to a surrender claim from the third country.

If the cloud provider processes personal data and is not only subject to the law of the GDPR, but also to the law of a third country that obliges it to disclose this personal data to government authorities of the third country in question, further determination activities are required by the evaluator that are similar comprehensive and appropriate to ensure the effectiveness of the additional measures taken by the cloud provider (e.g., document reviews, tests, inspections and audits).

As part of a document review, the documentation on the additional measures taken by the cloud provider to effectively protect the personal data from disclosure to the government authorities of the third country must be reviewed. If, for example, encryption and/or pseudonymization procedures are used, the documentation on the respective procedure(s) must be reviewed as part of the document review. With regard to the procedure in detail, the standards listed above for the additional measures for encryption and pseudonymization in the context of third-country transfers apply accordingly with regard to the document review.

In the case of technical measures, an evaluator should verify the effectiveness of the measures in the course of tests and inspections. If, for example, encryption and/or pseudonymization procedures are used or will be used, the effective implementation is to be determined and checked for adequacy as part of an inspection and/or test by representative random sampling. With regard to the procedure in detail, the above benchmarks listed for the additional measures on encryption and pseudonymization in the context of third-country transfers apply accordingly with regard to implementation.

Should pseudonymization procedures be used, verification of the effectiveness of the TOM taken to protect the additional identifiability information is also required to establish that control over the pseudonymization algorithm or the data store that enables re-identification from the additional information resides with a trusted entity (e.g., trustee) entrusted by the cloud provider and committed to confidentiality and located exclusively in a Member State or in a third country in the EEA or in a jurisdiction that offers a level of protection substantially equivalent to the EEA and therefore neither the pseudonymization algorithm nor the data store that enables re-identification based on the additional information is subject to a claim for return from the third country. The same applies to the use of encryption procedures for the storage of cryptographic key material.

In addition, evaluators can conduct interviews with employee on the previous handling of corresponding return requests from third countries (e.g., with regard to knowledge of the specified procedure).

No. 11.2 – Designation of a representative (Art. 27 in conjunction with Art. 3 (2) GDPR)

Criterion

(1) Cloud providers that do not have an establishment in the EU or the EEA but which are nonetheless subject to the General Data Protection Regulation under Art. 3 (2) GDPR, must designate a representative in the EU or the EEA in writing. The representative must be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or the behaviour of whom is monitored.

(2) The cloud provider assigns the representative with the task of acting as the point of contact for all issues related to data processing for the purpose of ensuring compliance with the General Data Protection Regulation and it must grant the representative the necessary authority to act in the name and on behalf of the cloud provider in order to fulfil the obligations of the General Data Protection Regulation.

Implementation guidance

The cloud provider can decide whether the representative should act in addition to the cloud provider or as the sole contact person; this is to be communicated accordingly in relation to third parties. If the cloud provider does not

have an establishment in the EU or the EEA and offers its service in several Member States, it does not have to appoint a representative in each Member State, instead it can appoint a representative in a Member State with responsibility for several Member States, provided that there are data subjects in this Member State.

Determination methods

- Document review

Determination activities

An evaluator performs a document review, checking, for example, contracts with representatives, appointment documents, policies, public information for cloud users (e.g., contact information of the representative on the website), responsibilities and their role descriptions. An evaluator performs a cross-check with the jurisdiction of the representatives (assigned member states) and the states in which cloud users are located. For this purpose, legally binding agreements with the cloud user and documents on the states in which the cloud service can be used can be consulted. Depending on the number of representatives, a sample check can be carried out.

C. Criteria and determination activities for processing as a controller

Chapter VII: The cloud provider as the controller

Explanation

As explained in A.1 'Addressees and function of the AUDITOR Criteria Catalogue', it may be necessary – depending on who the service is offered to – for the cloud provider to also process data of other data subjects such as the data of the employees of the cloud users (e.g., their names and contact details), besides the data of the cloud user, for the purpose of being able to provide the cloud service to the cloud user. This has the consequence that the cloud provider, in its role as the controller, does not only have to fulfil its data protection obligations towards the cloud user, but also towards the other data subjects.

If the cloud provider processes data of the cloud user to be able to provide the cloud service, it can invoke Art. 6 (1) subpara. 1 lit. b) GDPR, which permits the processing of personal data for the performance of a contract with the data subject or for taking steps at the request of the data subject prior to entering into a contract. However, the cloud provider cannot rely on this legal basis when processing, e.g., data of employees of the cloud user, because the employees are not contractual partners. Instead, the cloud provider can invoke Art. 6 (1) subpara. 1 lit. f) GDPR and its legitimate interests in the data processing, as long as the data processing is necessary for the business relationship with the cloud user.

With the exception of criterion no. 13, data processings based on Art. 6 (1) subpara. 1 lit. b) and lit. f) GDPR are summarised under "processing of personal data to provide the cloud service" for ease of reference, since they are equally necessary for the business relationship with the cloud user about the provision of the cloud service and can therefore be regarded as a unit.

No. 12 – Ensuring compliance with data protection principles (Art. 5 (1) and (2) in conjunction with Art. 24 GDPR)

Criterion

(1) The cloud provider must provide the data subject with all information it needs to verify the lawfulness of the processing of personal data, which are required for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations (principle of transparency).

(2) The cloud provider must define the purposes of each data processing clearly and precisely for the performance of the contract on the provision of the cloud service and fulfilling legal obligations (principles of purpose specification and purpose limitation).

(3) The cloud provider must define a process and it has put TOMs in place that ensure that personal data are processed only insofar as it is necessary (i.e., adequate, relevant and limited to the necessary extent) to achieve the specified purposes of the processing (principle of data minimisation).

(4) The cloud provider must define a process and it has put TOMs in place for verification of the factual accuracy, rectification, and erasure of inaccurate or incomplete personal data, which it processes for performing the contract on the provision of the cloud service and to fulfil legal obligations (principle of accuracy).

(5) The cloud provider must define a process and ensure by means of TOMs that data subjects can be identified during the data processing only for as long as this is necessary for achieving the specified purposes of the performance of the contract on the provision of the cloud service or the fulfilment of legal obligations, and must delete data that are no longer necessary as soon as possible. For this purpose, it sets criteria according to which the identification of data subjects is determined, maintained for the specified purposes of the processing, and made available to the required extent (scope and duration) for suitable storage (principle of storage limitation).

Explanation

The purpose represents the control parameter for the data selection and the process steps of the processing. Since a broad definition of the purpose specification hardly develops any controlling effect, it is not sufficient to merely determine the performance of the contract under Art. 6 para.(1) subpara. 1lit. b) GDPR or the fulfilment of legal obligations under Art. 6 (1) subpara.1 lit. c) GDPR as the purpose for data processing. Rather, the precise and specified business purpose and purposes of the processing must be determined for the purpose specification. The other data protection principles can develop their effects only once the purpose has been defined.

Personal data are adequate if they are appropriate from an objective perspective for the respective purpose in terms of function, content, and scope. Personal data are relevant if they make a difference for the fulfilment of the respective purpose, thereby decisively contributing to achieving the respective purpose. Personal data are limited to the necessary extent if the respective purpose of processing cannot be achieved without this data.

Implementation guidance

The principle of transparency is fulfilled if the cloud provider complies with obligations to provide information concerning the data processing (no. 15.1, no. 15.2, and no. 15.3). In addition, transparency, and data minimisation can be achieved by data protection by system design and by default (no. 19.1 and no. 19.2). When processing data for the provision of the service, the cloud provider should make and document considerations and decisions regarding the necessity of the data.

The cloud provider should establish and document TOMs for verifying, rectifying and erasing inaccurate or incomplete personal data for compliance with the principle of accuracy. These include, e.g., test procedures and erasure concepts, designation of a point of contact for cloud users for the receipt of requests, definition of responsibilities and procedural guidelines for prompt processing, and the specification of reporting channels. The TOMs can also be embedded in the existing customer support, troubleshooting or incident management systems.

To comply with storage limitation, the cloud provider should define storage periods for all data or categories of data, which are to be limited to the minimum necessary. In addition, periods should be set for erasing personal data or removing personal references. If data has to be stored due to legal regulations, it should be stored pseudonymously, and the personal reference should only be restored if necessary. Reference is made to the implementation guidance under no. 8.4 on data erasure.

Reference is made to the implementation guidance in SDM D1.1 to D1.8.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.5.2.1, 6.5.2.2, 7.2.1, 7.2.2 and 7.4.

Determination methods

- Document review
- Inspection
- Testing
- Auditing
- Development and design review

Determination activities

The fulfilment of the transparency principle is determined in the criteria on the information and disclosure obligations regarding data processing (No. 15.1 and No. 15.2) and the data protection-compliant system design and data protection-friendly default settings (No. 19.1 and No. 19.2).

In principle, an evaluator can gain access to TOMs, the documentation of data flows, the directory of processing activities and the data security concept in order to determine and ensure compliance with the data protection principles.

To determine compliance with the purpose specification and purpose limitation principles, an evaluator should perform a document review, including, for example, the privacy statement or TOM documentation that ensures logical or physical separation of data.

To ensure compliance with the principle of data minimisation and based on the analysis of the purpose limitation, a document review can be performed to check whether all collected and processed data are absolutely necessary for the processing. Here, an evaluator checks the process documentation of the cloud provider and the TOM used (e.g., authorisation concepts for access to personal data). Also, by means of an inspection, the data files held for the performance of the contract for the provision of the cloud service and for the fulfilment of legal obligations must be examined on a sample basis to determine whether they only contain data that is absolutely necessary for the achievement of the purpose.

An interview of the employees and the DPO with regard to procedural steps, processes and guidelines for data minimisation can also be carried out.

In support of this, a development and design review can determine whether the principles of data minimisation, purpose specification and purpose limitation are already incorporated during the development or design, so that only data necessary for the processing are processed, and, for example, corresponding data fields in databases and user interfaces are designed in a data-minimising manner.

An evaluator performs a document review to determine compliance with the principle of data accuracy. This includes, in particular, reviewing the process documentation to assess the factual accuracy, correction and deletion of inaccurate or incomplete personal data, as well as documentation on corresponding (technical) procedures (e.g., settings of database systems) and TOM for the correction and deletion of personal data, whereby reference is also

made here to the correction and deletion obligations (criteria no. 15.4 and 15.4). A test correction or deletion of data can be carried out as part of an inspection. An interview or observation of employees with regard to the verification, correction and deletion of inaccurate or incomplete personal data should be carried out (e.g., assessing their awareness of the procedural steps and guidelines, clear distribution of responsibilities).

To determine the principle of storage limitation, an evaluator performs a document review. In doing so, the evaluator examines, for example, deletion concepts (e.g., deadlines and type of deletion), documentation of measures taken such as pseudonymisation or anonymisation procedures to implement the principle of storage limitation, or protocols on deletions or pseudonymisations carried out. As part of an audit, employees should be interviewed about the limitation of data storage (e.g., questioning their knowledge about storage periods, guidelines, procedural steps).

No. 13 – Legal basis for data processing
(Art. 6 (1) subpara. 1 lit. b), c), or f) in conjunction with (2) GDPR)

Criterion

(1) The cloud provider may only process personal data and carry out processing operations that are necessary for the performance of a contract to which the cloud user is a party or for taking steps at the request of the cloud user prior to entering into a contract. The cloud provider must document structures and procedures leading to the conclusion of a contract or a pre-contractual relationship.

(2) The cloud provider may only process personal data and carry out processing operations that are necessary for compliance with a legal obligation under Member State or EU law to which the controller is subject. The cloud provider must document the legal obligations including the conditions of their occurrence, their scope, and the circumstances of their abolition.

(3) The cloud provider may only process personal data and carry out processing operations that are necessary for the purposes of its legitimate interests as relates to the fulfilment of the contract with the cloud user and where such interests in data processing are not overridden by the interests or fundamental rights and freedoms of the data subject. The cloud provider must document the process of balancing the interests, including the parties involved, whose interests are balanced, the specific interests, fundamental rights and freedoms, and the personal data and processing operations, the balancing criteria having been considered and the result of the balancing.

(4) The cloud provider must verify, determine, and document the legal basis for the processing operations pursuant to (1) to (3).

(5) The cloud provider must have instructions to employees based on which the existence of a sufficient legal basis is to be verified and it defines the corresponding responsibilities for reviews.

Explanation

AUDITOR considers the data processing operations of the cloud provider in its role as controller only to the extent necessary to fulfil the contract with the cloud user on the provision of the cloud service. The legal basis for data processing is therefore Art. 6 (1) subpara.1 lit. b) GDPR. It permits data processing insofar as it is necessary for the performance of a contract or taking steps prior to entering into a contract with the data subject. The handling of data for the conclusion of a contract, for making changes to the contract, and for the termination of the contract is part of the fulfilment of the contract. Data that are required to enable the use of the cloud service or to invoice the use of the cloud service is also part of the performance of the contract and therefore covered by Art. 6 (1) subpara.1 lit. b) GDPR.

If the cloud provider not only processes data regarding the cloud user for the performance of the contract with the cloud user, but also regarding other data subjects, e.g., the employees of the cloud user, then the cloud provider can invoke Art. 6 (1) subpara. 1 lit. f) GDPR and its legitimate interests, for as long as the data processing is necessary to perform the contract with the cloud user, and the interests, fundamental rights and freedoms of the data subject do not override the processing.

Where the cloud provider and cloud user conclude a contract on the provision of a cloud service, the cloud provider is obligated to process the cloud user's personal data, among other, based on retention duties under commercial and tax law. Art. 6 (1) subpara.1 lit. c) GDPR permits the data processing for compliance with a legal obligation to which the controller is subject. The actual legal basis for such processing follows from national or European regulations, since Art. 6 (2) GDPR contains an opening clause for the application of such regulations.

Processing operations that are based on the same legal basis can be summarised in their description, review and documentation.

Implementation guidance

Art. 13 (1) lit. c) or 14 (1) lit. c) GDPR (no. 15.1 or no. 15.2) oblige the cloud provider to inform the data subject of the legal basis of data processing. Therefore, the privacy policy of the cloud provider should not only clearly and precisely determine the purposes of the data processing under its own responsibility, but also specify the concrete legal basis for the data processing.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.15.1, 7.2.1 and 7.2.2.

Determination methods

- Document review, particularly legal analysis
- Inspection
- Testing

Determination activities

The evaluator checks the conclusion of standardised agreements to provide the service by reviewing a sample of agreements from the database (or other location of agreements). A sample comparison of the agreement conclusion date with the timestamp of the initial user record creation should also be performed. If no standardised agreements have been concluded, an evaluator checks all or a representative sample of legally binding agreements that a cloud provider has concluded with the cloud users for service provision as part of the document audit.

A representative sample should be selected at least so broad that a comparative assessment of a selection of agreements can rule out with a high degree of probability that another agreement deviates significantly. The sample size is therefore also dependent on the total number of agreements concluded. The individual agreements can be grouped together, whereby a sufficient number of agreements from each group of agreements must be examined. Agreements can be grouped according to, among other things, the subject matter, duration, nature and purpose of the processing.

In the case of data processing on the basis of Article 6 (1) (1) (b) GDPR, the evaluator performs a document review and checks the existence of concluded agreements on commissioned processing, samples thereof or notes on pre-contractual relationships entered into, on the basis of which data processing is carried out. Furthermore, the evaluator checks on a sample basis whether the data and processing operations processed by the cloud provider are necessary for the fulfilment of a contract for data processing on behalf of the cloud user or for the performance of pre-contractual measures. The determination activities for the principle of data minimisation from No. 12 apply analogously.

In addition, the evaluator must review suitable documentation (e.g., process documentation, function documentation, log files) to check whether the cloud provider has taken technical or organisational precautions to ensure an agreement conclusion before the actual service use (e.g., with regard to an agreement or registration process with potential cloud users). This function documentation must make it clear to an evaluator that a cloud service can only be provided if a legally binding agreement is concluded in accordance with the specifications of the criteria catalogue.

In support of this, an evaluator can perform an inspection in the form of a test execution of a corresponding agreement or registration process to ensure that the structures, processes and concepts specified in the documentation have also been implemented in the cloud service. As part of the trial service usage, an evaluator should also check whether the conclusion of an agreement can be circumvented by intent or misconduct.

In the context of a document review with representative samples, the evaluator checks whether the legal bases for the processing are laid down and communicated to the data subjects. For this purpose, the evaluator should examine the data protection declaration of the cloud provider, information notices to data subjects according to Art. 13 and 14 GDPR (see No. 15.1 and 15.2), the directory of processing activities according to Art. 30 (1) GDPR (see No. 18) and internal notes of the cloud provider from which the determination of a legal basis results.

In the context of a document review, the evaluator examines the instructions, guidelines, service instructions or similar documents to the employees of the cloud provider in which the procedure for checking the existence of a legal basis for the data processing by the employees is laid down, as well as the structures and responsibilities for such checks.

In the case of data processing on the basis of Article 6 (1) (1) (c) of the GDPR, the evaluator checks on a sample basis whether the data processed and processing operations by the cloud provider are necessary for the fulfilment of a legal obligation to which the cloud provider is subject. An evaluator can review documentation such as the description of the conditions of their occurrence, their scope and the circumstances of their elimination. The determination methods for assessing the principle of data minimisation from No. 12 apply analogously.

In the case of data processing on the basis of Art. 6 (1) (f) of the GDPR, the evaluator checks, as part of a sample document review, the specified process for weighing up interests. In addition, documents on interest assessments that have already been carried out can be examined on a sample basis in order to determine that they were carried out correctly. In support of this, an evaluator can carry out a test and inspection of the process of balancing interests to ensure that it is carried out in accordance with the process description.

No. 14 – Ensuring data security by means of appropriate state-of-the-art TOMs

Explanation

It also applies with regard to data processing for the performance of the contract with the cloud user on the provision of the cloud service and for the fulfilment of legal obligations that the cloud provider must ensure by means of TOMs that data are protected in accordance with their need for protection – above all, against security-relevant destruction, loss and unauthorised disclosure. Because the cloud provider will regularly not process personal data of protection category 3 by the performance the contract with the cloud user and for fulfilment of legal obligations, criteria are only given for protection categories 1 and 2.

No. 14.1 – Data security concept (Art. 24, 25, 32 in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

(1) The cloud provider must conduct a risk analysis with regard to data security and must maintain a data security concept that corresponds to its protection category and is appropriate for the specific risks of its data processing operations for the provision of the cloud service to the cloud user and fulfilment of legal obligations, which can result in particular from destruction, loss, alteration, unauthorised disclosure of and unauthorised access to personal data.

(2) The cloud provider must have a description of all data and data categories processed by it as a controller for providing the cloud service and fulfilling legal obligations.

(3) In addition to the data security concept, the information required in no. 14 can also be given in other documents, provided that as these have been legally bindingly agreed between the cloud provider and cloud user for the commissioned data processing. The requirements for the data security concept also apply to these other documents.

(4) In the data security concept, the cloud provider must specify which data security measures it has taken to eliminate or mitigate existing risks. The cloud provider must also describe the considerations it has made to arrive at these measures.

(5) The data security concept must be documented in writing or in an electronic form.

(6) The data security concept must be reviewed at regular intervals to ensure that it is up to date and appropriate and it must be updated as necessary.

(7) If the cloud provider involves processors for the performance of the contract with the cloud user, the data security concept must describe which data processing operations have been outsourced and are therefore subject to the processor's TOMs.

(8) If the data security concept requires security measures of the cloud user, these must be communicated to the cloud user in writing or in an electronic form.

Explanation

Risks of accidental and unlawful destruction, loss, alteration, unauthorised disclosure and unauthorised access to personal data must also be excluded or at least minimised with regard to data processing for the performance of the cloud service and fulfilment of legal obligations. In determining the specific measures, the cloud provider shall not only consider the processing modalities and the probability and severity of the damage, but also the state of the art and the costs for implementation of the measures. The considerations made must be made clear from the data security concept.

Implementation guidance

A risk analysis should also be carried out for the data processing operations for the performance of the contract with the cloud user and the fulfilment of legal obligations, which documents the risk assessment approach and methodology. Each risk should be addressed by one or more protective measures. The cloud provider can also use the implementation guidance under no. 2.1 for the creation and maintenance of the data security concept regarding the data processing for the performance of the contract with the cloud user and for the fulfilment of legal obligations.

Determination methods

- Document review, particularly legal analysis
- Inspection
- Auditing

Determination activities

For the determination of an appropriate data security concept, the determination activities in No. 2.1 apply analogously.

No. 14.2 – Security zone and entry control
(Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

(1) The cloud provider must protect premises and equipment from damage caused by acts of god[6] and must prevent unauthorised persons from gaining entry to premises and data processing equipment to prevent any knowledge being obtained of the personal data without authorisation and preclude any possibility of manipulating the data processing equipment. The TOMs must generally be appropriate for precluding entry by unauthorised persons due to technical or organisational errors, including operating errors of the cloud provider, or due to negligent acts by third parties. A minimum level of protection must be provided to make intentional interferences more difficult to achieve.

(2) The cloud provider must periodically review and, if necessary, update the timeliness and adequacy of the authorisations that are required for physical entry to rooms and equipment**.**

Protection category 2

(3) The criteria of protection category 1 must be fulfilled.

(4) In addition, the cloud provider must take appropriate measures not only to prevent damages in result of acts of god but also such in result of negligent acts of authorised persons. Physical entry must be adequately protected against intentional acts by unauthorised persons, which includes protection against entry attempts by means of known attack scenarios, deception and force.

(5) Every unauthorised entry and entry attempt must be detectable afterwards.

Explanation

Reference is made to the explanations in no. 2.2.

Implementation guidance

The implementation guidance under no. 2.2 is applicable.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

For determining access protection to premises and facilities, the determination activities in No. 2.2 apply analogously.

No. 14.3 – Admission control
(Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

(1) The cloud provider must ensure that unauthorised persons are not admitted to data processing systems and that they cannot manipulate them. This also applies to backups insofar as they contain personal data.

(2) The cloud provider must periodically review the current status and adequacy of rights that are required for admission to data processing systems and update them if necessary.

[6] Acts of god are unusual processes in nature that cannot be influenced by humans and are limited in time. Examples are lightning strikes, floods, and droughts.

(3) The cloud provider must protect the admission of authorised persons via the internet by means of a two-factor authentication procedure. Admission via the internet must occur via an encrypted communication channel.

(4) The measures for admission control must be appropriate to regularly prevent unauthorised persons from being admitted to data processing systems due to technical or organisational errors, including operating errors of the cloud provider, or due to negligent acts of the cloud user or third parties. A minimum level of protection must be provided to make intentional interferences more difficult to achieve.

Protection category 2

(5) The criteria of protection category 1 must be fulfilled.

(6) Protection measures must be in place against expected intentional unauthorised admission, which are capable of excluding expected admission attempts with sufficient certainty. The TOMs must ensure adequate protection against known attack scenarios as well as measures by which unauthorised admissions can normally be detected (afterwards).

Explanation

Reference is made to the explanations in no. 2.3.

Implementation guidance

The implementation guidance under no. 2.3 is applicable.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

The determination activities in No. 2.3 apply analogously to the examination of the admission control.

No. 14.4 – Access control
(Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

(1) The cloud provider must ensure by means of TOMs that authorised persons can only access personal data within the scope of their authorisation and must exclude unauthorised influences on data processing operations. This also applies to backups insofar as they contain personal data.

(2) The cloud provider must periodically review the current status and appropriateness of the rights that are required for access to personal data and update them if necessary.

(3) Any access to personal data must be controlled.

(4) The TOMs must be appropriate to regularly prevent access to data by unauthorised persons due to technical or organisational errors, including operating errors, of the cloud provider or due to acts of negligence of the cloud user or third parties. A minimum level of protection must be provided to make intentional interferences more difficult to achieve.

(5) The cloud provider must protect access by authorised persons via the internet by means of a two-factor authentication.

Protection category 2

(6) The criteria of protection category 1 must be fulfilled.

(7) Protection must be provided against expectable intentional unauthorised access, which is capable of excluding expectable attempted access with sufficient certainty. The TOMs must ensure adequate protection against known attack scenarios as well as measures by which unauthorised admissions can normally be detected (afterwards).

Explanation

Reference is made to the explanations in no. 2.4.

Implementation guidance

The implementation guidance under no. 2.4 is applicable.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

The determination activities in No. 2.4 apply analogously to the examination of access control.

No. 14.5 – Transfer of data and transport encryption
(Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) and (2) GDPR)

Criterion

Protection category 1

(1) The cloud provider must use state-of-the-art transport encryption or equally appropriate measures for data transfer processes or configure interfaces in such a manner that this is a requirement. The transport encryption used must ensure that personal data cannot be read, copied, modified, or deleted without authorisation during electronic transfers. The encryption keys for an encrypted transmission must be stored securely.

(2) The cloud provider must regularly prevent such acts of unauthorised persons due to technical or organisational errors, including operating errors, of the cloud provider or its employees or due to negligent acts by the cloud user or third parties. The TOMs regularly prevent the negligent disclosure of data to unauthorised persons by the cloud provider and its employees. A minimum level of protection must be provided to make intentional interferences more difficult to achieve.

(3) The cloud provider must automatically log the metadata of all data transfer operations, including those of recipients and those from and to the cloud user or sub-processor.

(4) The criteria also apply to the transfer of data within the cloud provider's own network and that of its processors and between them.

(5) During the transport of data media, the cloud provider must use TOMs to prevent personal data from being read, copied, modified, or deleted without authorisation. The cloud provider must keep records of the transports.

Protection category 2

(6) The criteria of protection category 1 must be fulfilled.

(7) The cloud provider must protect the personal data from intentional unauthorised reading, copying, alteration, or deletion and must exclude expectable attempts with sufficient certainty. The cloud provider must protect against known attack scenarios and normally detects any unauthorised reading, copying, alteration, or deletions (afterwards).

Explanation

Reference is made to the explanations in no. 2.5.

Implementation guidance

The implementation guidance under no. 2.5 is applicable, whereas reference is made to no. 7.4.9 instead of no. 8.4.3 of ISO/IEC 27701.

Determination methods

- Document review
- Testing
- Auditing

Determination activities

The evaluator can verify the protection of data-in-transit analogously to No. 2.5.

No. 14.6 – Traceability of data processing (Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. c), e), f) and (2) GDPR)

Criterion

Protection category 1

(1) The cloud provider must log entries, alterations, and erasures of data that are required for the performance of the contract for the provision of the cloud service or for the fulfilment of legal obligations to ensure that data processing can be verified and traced afterwards. The principles of necessity, purpose limitation, and data minimisation must be observed for the logging. Log data must be stored securely.

(2) The cloud provider can trace data entries, alterations, and erasures at any time, which are made in the course of the intended use of the cloud service by the cloud user or during administrative measures of the cloud provider.

(3) The cloud provider must design the logs of the administrative activities and user activities in such a way that entries, alterations, and erasures can generally be traced even in the event of technical or organisational errors, including operating errors of the cloud provider or its employees or negligent acts by the cloud user or third parties. The cloud provider must provide a minimum level of protection against intentional manipulation of the traceability measures, which makes such manipulation more difficult.

Protection category 2

(4) The criteria of protection category 1 must be fulfilled.

(5) The cloud provider must provide protection against expactable intentional manipulation of logging instances and against intentional access to or manipulation of logs by unauthorised persons, whereby expectable manipulation attempts are prevented with sufficient certainty. These protection measures must include in particular adequate protection against known attack scenarios as well as measures by which manipulation can normally be detected (afterwards).

Explanation

Reference is made to the explanations in no. 2.6.

Implementation guidance

The implementation guidance under no. 2.6 is applicable. Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.8.

Determination methods

- Document review, particularly legal analysis
- Inspection
- Testing
- Auditing

Determination activities

The comprehensibility of the data processing can be checked by the evaluator analogously to No. 2.6.

No. 14.7 – Encrypting stored data (Art. 32 (1) lit. a) GDPR)

Criterion

Protection category 1 and 2

(1) The cloud provider must ensure that login data for the use of the cloud service is stored in encrypted form.

(2) Personal data that must be stored for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations must be stored in encrypted form.

(3) The cloud provider must continuously monitor technical developments relating to encryption and must use encryption procedures compliant with best practice standards.

(4) Implemented encryption procedures are to be replaced by other encryption procedures when they are no longer compliant with best practice standards.

Explanation

In addition to pseudonymisation, encryption of personal data is explicitly mentioned in Art. 32 (1) lit. a) GDPR as a security measure to be implemented. The purpose of encryption is to ensure the protection goals of confidentiality and integrity (SDM C1.4 and C1.3). The threshold above which encryption is required is low. This results in the consequence that personal data should be encrypted whenever possible, even if there is only a low risk.

Implementation guidance

The implementation guidance under no. 2.9 for protection category 2 is applicable.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

The determination activities under No. 2.9, protection category 2 apply analogously to the testing of encrypted storage.

No. 14.8 – Separate processing
(Art. 5 (1) lit. b) in conjunction with Art. 24, 25, 32 (1) lit. b) and (2) GDPR)

Criterion

Protection category 1

(1) Personal data that is processed for the performance the contract on the provision of the cloud service or for the fulfilment of legal obligations must be processed separately by the cloud provider and in accordance with the respective purposes of the processing.

(2) Data separation must commonly be maintained, even in the event of technical or organisational errors, including operating errors, of the cloud provider or its employees. The cloud provider must provide a minimum level of protection to prevent intentional violations of the separation principle.

Protection category 2

(3) The criteria of protection category 1 must be fulfilled.

(4) The cloud provider must exclude expectable intentional violations with sufficient certainty. In the context of data storage, the TOMs required to this end must include encryption with individual keys. The cloud provider must normally detect intentional violations of the separation principal (afterwards).

Explanation

The criterion promotes the protection goals of availability, integrity, confidentiality, and unlinkability (SDM C1.2 – C1.5), thereby also aiming to secure the principle of purpose limitation under Art. 5 (1) lit. b) GDPR.

Implementation guidance

The implementation guidance under no. 2.10 is applicable. Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.8.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

Data separation and its adequacy can be checked by the evaluator analogously to No. 2.10.

No. 15 – Safeguarding the rights of the data subject

Explanation

If the data subject exercises his rights according to Art. 15-22 GDPR by electronic means, the information on actions taken in response to the request should also be provided by electronic means where possible, in accordance with Art. 12 (3) sent. 4 GDPR, unless the data subject has requested another information channel. It should be noted, however, that Art. 20 to 22 GDPR are not considered in Chapter D in the AUDITOR certification.

No. 15.1 – Information to be provided where personal data are collected from the data subject (Art. 13 in conjunction with Art. 12 (1) and Art. 5 (1) lit. a) GDPR)

Criterion

The cloud provider must ensure by means of TOMs that it informs the data subjects at the time of the collection of its personal data for the performance of the contract on the provision of the cloud service and for the fulfilment of legal obligations about the circumstances of the processing and their rights as data subjects in an intelligible form using clear and plain language. The cloud provider must inform the data subject of all information required under Art. 13 (1) and (2) GDPR.

Explanation

Pursuant to Art. 13 GDPR, the cloud provider is obligated to inform the data subjects of the circumstances of the direct data collection. This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Implementation guidance

The cloud provider should provide the cloud user with its privacy policy containing all information under Art. 13 (1) and (2) GDPR when registering for the use of the cloud service (e.g., via the website or the information portal of the cloud service). The cloud provider should provide a point of contact for the cloud user with appropriate availability and authorisations, who can initiate the immediate fulfilment of the rights of the data subject.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.1, 7.3 and 7.5.

Determination methods

- Document review
- Inspection

Determination activities

The evaluator checks the template privacy policy with the information pursuant to Art. 13 (1) and (2) GDPR, which the cloud user receives upon the conclusion of the contract for the provision of the cloud service. If the contract is concluded online, it can be checked within the scope of a (test) contract conclusion whether the cloud provider provides all information pursuant to Article 13 (1) and (2) GDPR. To check the duty to inform other data subjects, such as the employees of the cloud user, the evaluator also checks the template privacy policy that the cloud provider sends to the employee, for example, via e-mail when the data is collected.

No. 15.2 – Information to be provided where personal data have not been obtained from the data subject (Art. 14 in conjunction with Art. 12 (1) and Art. 5 (1) lit. a) GPPR)

Criterion

If personal data have not been obtained directly from the data subject for the performance of the contract on the provision of the cloud service and for the fulfilment of legal obligations (third-party collection), the cloud provider must ensure by means of TOMs that the data subject is informed, within an appropriate period and in an intelligible form, using clear and plain language, about the circumstances of the processing and the rights of the data subjects, unless the provision of such information is impossible or would involve a disproportionate effort. The information to the data subject must include all information required pursuant to Art. 14 (1) and 2 GDPR.

Explanation

This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C.2.7).

Implementation guidance

The cloud provider should ensure the allocation of responsibilities and reporting channels, and document these to be able to inform the data subject in a timely manner. The appropriateness of the period for providing information is based on the specific circumstances of the processing. According to Art. 14 (3) lit a) GDPR, the period is at the latest one month after obtaining the personal data. Shorter periods apply if the personal data are to be used for

communication with the data subject or be disclosed to other recipients. In the first case, Art. 14 (3) lit. b) GDPR, the cloud provider must comply with its obligation to provide information at the latest at the time of the first communication to that data subject. In the second case, the information can be provided according to Art. 14 (3) lit. c) GDPR at the latest when the personal data are first disclosed to the recipient.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.1, 7.3 and 7.5.

Determination methods

- Document review

Determination activities

The evaluator examines the template privacy policy with the information according to Article 14 (1) and (2) GDPR that the cloud provider makes available to the data subject. In addition, the evaluator examines documentation on the notification procedure, for example, procedural steps, notification channels or protocols on notifications carried out.

No. 15.3 – Access to information (Art. 15 in conjunction with Art. 5 (1) lit. a), 3rd alt. GDPR)

Criterion

> The cloud provider must ensure by means of TOMs that it grants the data subject access to the personal data upon request that it processes as the controller for the performance of the contract on the provision of the cloud service and for the fulfilment of legal obligations. The cloud provider must provide a copy of this data to the data subject.

Explanation

This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Implementation guidance

Pursuant to Art. 12 (3) GDPR, the cloud provider is to provide the data subject access to his data without undue delay and in all cases within one month of receipt of the request. The request process should be as simple as possible, which is why contact forms or customer self-services should be provided via an online platform. Pursuant to Art. 15 (3) GDPR, the data subject has the right to receive a copy of the personal data undergoing processing.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.3.1, 7.3.2, 7.3.3, 7.3.6, 7.3.8 and 7.3.9.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documentation on measures for providing information to a cloud user. In particular, the evaluator should be given access to the documentation of the relevant mechanisms and reporting channels, service descriptions. An evaluator should review exemplary records and logs of instructions given and subsequent information provided.

As part of an inspection, a representative sample disclosure can be carried out to check whether disclosure and provision of the data are possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). During an audit, interviews (e.g., to gain knowledge of procedural steps, etc.) and observations can also be used to check whether information can be provided in response to a request.

No. 15.4 – Rectification and completion (Art. 16 in conjunction with Art. 5 (1) lit. d) GDPR)

Criterion

> The cloud provider must ensure by means of TOMs that it grants data subjects the possibility to correct or erase any incomplete or inaccurate personal data relating to the provision of the cloud service on their own. Alternatively, the cloud provider must perform the (legitimate) rectification or erasure.

Explanation

The cloud provider is obligated under Art. 16 GDPR to rectify inaccurate personal data and to complete incomplete personal data of data subjects upon request. The rectification pursuant to Art. 16 GDPR promotes the protection goal of intervenability (SDM C1.7).

Implementation guidance

The cloud provider is also responsible for the accuracy of data in accordance with Art. 5 (1) lit. d) GDPR, irrespective of the data subject's request, which is why it should set periods for the regular review and rectification of data.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.3.1, 7.3.2, 7.3.6 and 7.3.9.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documentation of actions taken to correct and complete data (e.g., documentation of relevant mechanisms and reporting channels, service descriptions). An evaluator should review sample records and logs of user instructions given and subsequent corrections or completions.

As part of an inspection, a representative sample correction and completion can be carried out to check whether rectification and completion of data are possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). During an audit, interviews (e.g., to gain knowledge of procedural steps, etc.) and observations can also be used to check whether a correction or completion can be carried out.

No. 15.5 – Erasure
(Art. 17 (1) GDPR)

Criterion

(1) The cloud provider must ensure by means of TOMs that it erases personal data processed by it for the performance of the contract on the provision of the cloud service upon request by the data subject and on its own initiative without undue delay when the requirements of Art. 17 (1) lit. a), d) or e) GDPR are met. The erasure must be unrecoverable, so that no information about the data subject can be obtained from the erased personal data, even when employing relatively great effort.

(2) The cloud provider must ensure that the personal data processed by it for the performance of the contract on the provision of the cloud service is not only erased from the active data base, but also from copies and data backups.

(3) The cloud provider must ensure that the erasure will be repeated for the relevant data after data are recovered, which have already been erased from the active data base but not from the data backup yet.

Explanation

The criterion promotes the protection goals of intervenability and unlinkability (SDM C1.7 and C1.5). In particular, there is no obligation to erasure if the cloud provider is obligated to process the data for compliance with a legal obligation (Art. 17 (3) lit. b) GDPR).

Since Art. 17 GDPR is based on an unrecoverable erasure, measures of logical erasure such as the removal of personal data from directories by erasure commands are not sufficient to meet the requirements of Art. 17 GDPR.

It is referred to the implementation guidance under ISO / IEC 27701 no. 7.3.1, 7.3.6, 7.3.9 and 7.4.7.

Implementation guidance

To be able to comply with its erasure obligations, the cloud provider should create an erasure concept by means of which it can continuously determine and check its erasure obligations. The erasure concept should include criteria that can be used to determine whether a data record must be erased or stored due to retention periods. Metadata such as the purpose of the processing, the definition of indicators for the loss of statutory permissions, retention periods, and the legal basis for the storage should therefore be laid down for each data record.

Since the erasure of data in backup and fail-safe systems is more time-consuming than erasure from the active database, copies and data from backup systems can also be erased at later points in time from active database, e.g., in the course of overwriting or destroying the affected data media. As a rule, the erasure in the backup files should take place no later than one year after erasure in the active database, whereas it should be aimed for shorter periods.

The implementation guidance under no. 6.4 is applicable.

Determination methods

- Document review
- Inspection
- Testing
- Auditing

Determination activities

The evaluator checks documentation on measures for the erasure of data (e.g., documentation of relevant mechanisms and reporting channels, deletion concepts, requirements and deadlines for deletion, service descriptions). An evaluator can also check the (automated) notification of actual deletions of personal data no longer needed for service provision.

During an inspection, a representative sample deletion can be carried out to check whether a (complete) deletion of data is possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). During an audit, it can also be checked on the basis of interviews (e.g., assessing employees' knowledge of procedural steps, etc.) and observations whether a deletion can be carried out.

Supporting security tests can be carried out to check that data has been deleted in a sufficiently secure manner.

The possibilities for determination activities under No. 6.4 are applicable.

No. 15.6 – Restriction of processing (Art. 18 (1) and (3) GDPR)

Criterion

(1) The cloud provider must ensure by means of TOMs, that, upon the data subject's request, it can restrict the processing of personal data processed by it for the performance of the contract with the cloud user on the provision of the cloud service or for the fulfilment of a legal obligation.

(2) The cloud provider must ensure by means of TOMs that it informs the data subject before the restriction of processing is lifted.

Explanation

Pursuant to Art. 18 (1) GDPR, the cloud provider is obligated to restrict the processing of personal data under certain conditions, so that the data cannot be further processed or modified. The criterion promotes the protection goal of intervenability (SDM C1.7).

Implementation guidance

A restriction of processing can be implemented, for example, by a temporary transfer to another processing system or by blocking.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.3.1, 7.3.2, 7.3.3 and 7.3.9.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documentation of measures taken to restrict the processing of data (e.g., documentation of relevant mechanisms and reporting channels, service descriptions, measures to inform the cloud user). An evaluator should review exemplary records and logs of instructions given and subsequent restrictions. Messages or protocols on the lifting of restrictions to cloud users can also be examined.

Within the scope of an inspection, a representative restriction can be carried out to check whether a restriction on data processing and the cancelation of this (including notification to the cloud users) is possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). During an audit, interviews (e.g., to gain knowledge of procedural steps, etc.) and observations can also be used to check whether a restriction or informing the cloud user about a cancelation of the restriction can be carried out.

No. 15.7 – Notification obligation in the event of rectification, erasure or restriction of processing

(Art. 19 in conjunction with Art. 5 (1) lit. a) 3rd alt. GDPR)

Criterion

Insofar as the cloud provider has disclosed to recipients data subject's personal data processed by it for the performance of the contract with the cloud user on the provision of the cloud service or due to legal obligations, it must ensures by means of TOMs that it communicates every rectification or erasure of personal data and every restriction of processing to each recipient and informs the data subject about the recipients if the data subject so requests.

Explanation

The cloud provider is obligated under Art. 19 GDPR to notify recipients – to whom it has disclosed personal data – of any rectification, erasure, or restriction of processing and to inform the data subject of the recipients upon request. The criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Recipients are, for example, processors that are engaged for the performance of the contract on the provision of the cloud service.

Reference is made to the implementation guidance of ISO/IEC 27701 no. 7.3.1, 7.3.2, 7.3.3, 7.3.7 and 7.3.9.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documentation on communication actions (e.g., documentation of relevant mechanisms and reporting channels, service descriptions). An evaluator should review exemplary records and logs of instructions given and subsequent notification. An evaluator can also check whether cloud users have already requested notification of recipients, and if so, how a cloud provider has handled this request.

In the course of an inspection, test restrictions (including notification of the person concerned) and the cancelation of these can be carried out. The restriction can be carried out, for example, by a technical function within the cloud service or by manual requests to the cloud service support. In the context of an audit, interviews (e.g., to gain knowledge of procedural steps, etc.) and observations can also be used to demonstrate how restrictions and their removal are carried out and how the affected person is notified.

No. 15.8 – General information obligation, information obligation in the event of inaction or delayed request processing
(Art. 12 (3) and (4), Art. 15 to 19 GDPR)

Criterion

(1) The cloud provider must ensure by means of TOMs that it informs the data subject on actions taken on request under Art. 15 to 19 GDPR as relates to the data processing performed by it as the controller for the performance of the contract on the provision of the cloud service and for fulfilment legal obligations, without undue delay, whereas at the latest within one month after receipt of the request.

(2) The cloud provider must ensure by means of TOMs that it informs the data subject if it does not answer his request in accordance with Articles 15 to 19 GDPR as relates to the data processing performed by it as the controller for the performance of the contract on the provision of the cloud service and for fulfilment legal obligations, without undue delay, whereas at the latest within one month. The information refers to the extension of the period and the reasons for this.

(3) The cloud provider must ensure by means of TOMs that it informs the data subject, at the latest within one month, if it does not take action to answer its request in accordance with Art. 15 to 19 GDPR as relates to the data processing performed by it as the controller for the performance of the contract on the provision of the cloud service and for fulfilment legal obligations. The information of the data subject must refer to the reasons for inaction and the possibility to lodge a complaint with the supervisory authority or to seek a judicial remedy.

Explanation

According to Art. 12 (3) sent. 1 GDPR, the cloud provider has to provide the data subject with the necessary information on actions taken on a request under Art. 15 to 22 GDPR without undue delay, whereas at the latest within one month after receipt of the request. Art. 20 to 22 GDPR are not considered in Chapter D in the AUDITOR certification. The cloud provider, therefore, has to respond to the requested action on each request from a data

subject pursuant to Art. 15 to 19 GDPR. If the cloud provider relies on a (national) exception to the rights of the data subject when answering requests, it must therefore adequately explain the reasons to the data subject for rejecting his request in part or in full.

Due to the complexity or the number of the requests, the one-month period under Art. 12 (3) sent. 1 GDPR can be extended by two months. In this case, the cloud provider is to inform the data subject about the extension of the period and the reasons for this in accordance with Art. 12 (3) sent. 3 GDPR. If the request is made by electronic means, the information should also be provided by electronic means, unless otherwise requested by the data subject.

Art. 12 (4) GDPR obligates the cloud provider to inform the data subject, at the latest within one month, of the reasons why it does not, despite a request pursuant to Art. 15 to 19 GDPR, take action to comply with the request. Reasons not to comply with a request are, e.g., unfounded or excessive requests according to Art. 12 (5) sent. 2 lit. b) GDPR. Furthermore, according to Art. 12 (4) GDPR, the data subject must be informed of his option to lodge a complaint with the supervisory authority pursuant to Art. 77 GDPR or to seek a judicial remedy pursuant to 79 GDPR.

Implementation guidance

The cloud provider should express, as concisely, intelligibly and clearly as possible, which actions it has taken to comply or not to comply with the request of the data subject. Especially if the request of a data subject has been partially or completely rejected, the reasons for this should be described as detailed as possible, so that the data subject can assess whether it would like to take actions against the cloud provider (e.g., a complaint to the supervisory authority).

It should also be expressed, as concisely, intelligibly and clearly as possible, why a longer period is required for processing the request and this period should be specified. The same applies to naming the reasons for inaction.

Determination methods

- Document review
- Inspection
- Auditing

Determination activities

The evaluator examines documents on measures taken by a cloud provider to provide the required information to a data subject. Process documentation and logs can be used to verify that the information is provided to the data subjects, including the completeness of the information provided and its timely provision.

During an inspection, the evaluator can carry out a sample information provision to check that this is possible and provides all the required information.

An audit may also include an interview with relevant staff (e.g., to understand the established process for responding to data subjects' requests or the reasons for not responding to data subjects' requests).

No. 16 – Notification of personal data breaches (Art. 33 (1), (3) to (5) GDPR)

Criterion

(1) The cloud provider must have a process in place for notifying personal data breaches arising from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, including the definition of procedural steps, deadlines and measures for the identification, analysis, and evaluation of the personal data breach and its reporting, the responsibilities, and the awareness-raising of the employees involved.

(2) The cloud provider must notify the supervisory authority without undue delay as soon as it becomes aware of personal data breaches arising from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, if the personal data breach is unlikely to result in a risk to the rights and freedoms of the cloud user.

(3) The cloud provider must maintain a process and measures to identify, analyse, and evaluate the risk to the rights and freedoms of the data subjects.

(4) The cloud provider must document any personal data breaches, including the facts relating to the personal data breach, its effects, and the remedial actions taken.

(5) The notification to the competent supervisory authority must include at least the requirements set out in Art. 33 (3) lit. a) to d) GDPR.

(6) The cloud provider must determine which factors must be fulfilled so that for making an assumption that a risk to the rights and freedoms of the cloud user can be expected and the person who is responsible for the notification. The competent employees must be sufficiently trained to be able to assess violations.

Explanation

The cloud provider is obligated to notify personal data breaches to the supervisory authority under Art. 33 GDPR without undue delay insofar as they are likely to result in a risk to the rights and freedoms of natural persons. The cloud provider must document personal data breaches in a manner enabling the supervisory authority to verify the cloud provider's compliance with the requirements of this Article. The criterion promotes the protection goal of integrity and transparency (SDM C1.3 and C1.6).

Implementation guidance

The cloud provider should establish and document corresponding processes, as well as define contact persons, responsibilities and reporting channels. The notification of personal data breaches should be integrated in the incident and troubleshooting management of the cloud provider to enable processing in a timely manner.

Reference is made to the implementation guidance in BSI C5 SIM-01 to SIM-07.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.13.1.

Official reporting forms can be used to notify personal data breaches to the supervisory authority.

Determination methods

- Document review
- Auditing

Determination activities

An evaluator examines the data security concept and the TOMs described therein for the notification of data security breaches. The evaluator may also review other documentation, including, for example, process documentation with the procedural steps and deadlines for data breach notification, process directories, process instructions, guidelines, templates for data breach notification, decision rules for assessing data breaches, risk assessment procedures and factors included in the risk analysis, reporting channels and responsibilities/competences.

As part of a document review, data breach notifications already submitted to the data protection supervisory authority can also be checked for completeness in accordance with Article 33 (3) GDPR, if they exist. In the case of reported data breaches, the documentation of the TOM for remedying the data breach should also be examined in particular with regard to its suitability and protective effect for remedying the data breach or mitigating the adverse effects, as well as whether the 72-hour deadline was met and, if not, how the extension of the deadline was justified.

The implementation of these concepts can be tested by interviewing employees or observing the conduction of a sample report. An on-site audit should examine whether sufficient resources are available to ensure that reports are processed quickly.

An evaluator should also examine documents on the training of responsible staff (e.g., certificates, evidence of workshops) and interview them (e.g., with regard to awareness of policies and procedures) as part of an audit. The evaluator can also check the organisation chart or an overview of staff responsibilities with corresponding documented staff qualifications. In doing so, the evaluator must also check through interviews whether responsibilities are clearly communicated and regulated (e.g., who is responsible for deciding on and making the notification to the supervisory authority).

No. 17 – Communication of a personal data breach to the data subject (Art. 34 (1) to (3) GDPR)

Criterion

(1) The cloud provider must communicate personal data breaches to the data subject without undue delay, which arise from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject.

(2) The communication must contain at least the information under Art. 33 (3) lit. b), c) and d) GDPR in clear and plain language.

(3) The cloud provider must maintain a procedure for the identification, analysis, and evaluation of personal data breaches arising from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, based on which it is determined which factors must be fulfilled so that a high risk to the rights and freedoms of the data subject can be assumed, which deadlines are to be observed, and the person who is responsible for the communication. The competent employees must be sufficiently trained to be able to assess violations.

(4) The communication according to (1) and (2) may be omitted if the requirements of Art. 34 (3) GDPR are met.

(5) The cloud provider must document the communications of data subjects about personal data breaches arising from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, and of the circumstances, reasons, and measures when the communication to data subjects in accordance with (4) does not take place.

Explanation

A high threat level, which requires communication to the data subject in accordance with Art. 34 GDPR, can be assumed, for example, in the event that bank and credit card information are lost. Such data are often processed for the purpose of performing the contract with the cloud user, whereby the obligation to communicate personal data breaches may become relevant.

The communication to the data subject referred to in Art. 34 (1) GDPR is not required in accordance with Art. 34 (3) GDPR if one of the following conditions is met:

a. the controller has implemented appropriate technical and organisational protection measures, and these measures were applied to the personal data affected by the personal data breach, in particular such measures that render the personal data unintelligible to any person who is not authorised to access it, e.g., by encryption;

b. the controller has taken subsequent measures, which ensure that the high risk to the rights and freedoms of data subjects referred to in (1) is no longer likely to materialise;

c. the communication would involve disproportionate effort. In such a case, there a public communication or similar measure is to be implemented, whereby the data subjects are informed in an equally effective manner.

Implementation guidance

The implementation guidance under no. 8.2 is applicable, whereas reference is made to no. 7.3.1 and 7.3.2 instead of no. 8.2.5 and 8.3 of ISO/IEC 27701.

Determination methods

- Document review
- Auditing
- Inspection

Determination activities

An evaluator examines the data security concept and the TOM described therein for the notification of data protection breaches. The evaluator may also review other documentation, including, for example, the process documentation with the procedural steps and deadlines for notifying data subjects of data breaches, procedure directories, procedure instructions, guidelines, samples and templates for notifying data subjects of data breaches, decision rules for assessing data breaches, procedures for risk assessment and factors to be included in the risk analysis, as well as reporting channels and responsibilities.

As part of a document review, notifications of data breaches already sent to data subjects can also be checked for completeness of the minimum content according to Article 33 (3) (b), (c) and (d) GDPR and comprehensibility for the data subjects, if such exist.

If the cloud provider has refrained from notifying data subjects of data breaches in the past, the evaluator shall check the existence of the requirements according to Art. 34 (3) GDPR. As part of a document review (e.g., the documentation in the data security concept), the evaluator must check which TOMs the cloud provider has taken and whether these are suitable so that there will probably no longer be any high risks to the rights and freedom of the data subjects in the future. The documentation should also show which risks are addressed by the measures. Technical measures can be examined by the evaluator in the course of an inspection. In the case of Art. 34 (3) (c) GDPR, the evaluator will examine the documentation of the public notification, for example, in a daily newspaper that was carried out instead of individual notification of the data subjects, and the explanation of the disproportionate effort of individual notification.

Whether the established procedure for the identification, analysis and evaluation of data protection breaches is practised by the cloud provider can also be carried out by interviewing employees (e.g., with regard to the awareness of policies and procedural steps). In doing so, the evaluator must also check through interviews whether responsibilities are clearly communicated and regulated (e.g., who is responsible for deciding on and carrying out the notification of the affected persons). An observation of a trial notification can also be carried out.

The competence of staff should be verified by examining documentation of skills (e.g., certificates) or training provided and through staff interviews. The evaluator can also check the organisation chart or an overview of the staff responsibilities with corresponding documented staff qualifications.

No. 18 – Maintaining a record of processing activities (Art. 30 (1), (3) to (5) GDPR)

Criterion

(1) If the cloud provider is obligated to maintain records of processing activities, this record must refer to the processing activities that it carries out for the performance of the contract on the provision of the cloud service legal obligations. The record must also contain the content listed in Art. 30 (1) lit. a) to g) GDPR.

(2) The cloud provider must maintain a process for updating the record of processing activities if processing activities are introduced or eliminated, or if the information according to Art. 30 (1) lit. a) to g) GDPR changes for the listed processing activities.

(3) For the purpose of updating the record of processing activities, the cloud provider must maintain processes for cooperation between the specialist operational departments involved in the processing activities, its representative and, if applicable, the DPO and must regulate the internal responsibilities for this.

(4) The record of processing activities must be maintained in writing, including in electronic form and the storage locations must be known.

(5) The record of processing activities must be made available to the supervisory authority upon request. The cloud provider must maintain processes for receiving, processing, and answering requests from supervisory authorities and must regulate the internal responsibilities for this.

(6) If the cloud provider is obligated to designate a representative and maintain a record of processing activities, it must ensure that the representative also keeps the record of processing activities and complies with the criteria according to (1) to (5).

Explanation

The criterion promotes the protection goal of transparency (SDM C1.6).

As a rule, cloud providers with more than 250 employees are obligated to maintain records of processing activities. However, cloud providers with fewer employees who process data to provide the cloud service to the cloud user generally also have to maintain records of processing activities, since this processing takes place regularly and not only occasionally, so that the exception under Art. 30 (5) GDPR is not applicable.

According to Art. 30 (2) GDPR, the representative of the cloud provider, if one is designated, must also maintain a record of processing activities.

Implementation guidance

The implementation guidance under no. 8.3 is applicable.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.8.

Determination methods

- Document review
- Auditing

Determination activities

The evaluator may check the maintenance of a record of processing activities analogously to No. 8.3.

No. 19 – Data protection by design and by default

No. 19.1 – Data protection by system design (Art. 25 (1) in conjunction with Art. 5 (1) and (2) GDPR)

Criterion

Within the framework of the service design, the cloud provider must conduct a risk analysis and ensure by means of TOMs that only personal data necessary for the performance of the contract on the cloud service processed in the cloud service and that the remaining principles of Art. 5 GDPR are implemented in the cloud service.

Explanation

While the cloud provider, in its role as the processor, is only an indirect addressee of Art. 25 GDPR, the cloud provider as the controller is a direct addressee. The cloud service technology and organisation must be designed in such a way that they support the data protection principles of Art. 5 GDPR in the best possible way. The cloud provider must ensure that it only processes personal data that are necessary for the provision of the service to the cloud user when designing the service. The extent of the processing of the data and the storage period must be limited to what is necessary to achieve the purpose of processing.

Implementation guidance

The implementation guidance under no. 9.1 is applicable, whereas reference is made to no. 7.4 instead of no. 8.4 of ISO/IEC 27701.

Determination methods

- Document review
- Inspection
- Testing
- Auditing
- Development and design review

Determination activities

For the examination of data protection by system design, the determination activities in No. 9.1 apply analogously.

No. 19.2 – Data protection by default (Art. 25 (2) in conjunction with Art. 5 (1) and (2) GDPR)

Criterion

(1) The cloud provider must ensure by default setting that only personal data that are necessary for providing the cloud service are processed for the initial start-up and use of the cloud service and the access to personal data is also limited to what is necessary.

(2) The cloud provider must ensure by default settings that personal data are not made accessible to an indefinite number of natural persons without the data subject's intervention.

Implementation guidance

The implementation guidance under no. 9.2 is applicable. Instead of the no. 8.4 of ISO/IEC 27701 referred to in no. 9.2, no. 7.4 is applicable.

Determination methods

- Document review
- Inspection
- Testing
- Auditing
- Development and design review

Determination activities

For the examination of data protection through data protection-friendly default settings, the determination activities in No. 9.2 apply analogously.

For the examination of the necessity of data processing, the determination activities in No. 12 on the basic principle of data minimisation apply analogously.

No. 20 – Order processing by the cloud provider

Explanation

The data processing necessary for the performance of the contract with the cloud user on the cloud service does not have to be performed by the cloud provider personally. Rather, the cloud provider can also outsource data processing to processors (e.g., for invoicing the cloud usage to the cloud user); as such, this outsourcing must also be included in the certification examination.

No. 20.1 – Services governed by a legally binding agreement (Art. 28 (3) subpara. 1 sent. 2 GDPR)

Criterion

(1) Where the cloud provider outsources the processing of data necessary for the performance of the contract on the cloud service to a processor, it must conclude a legally binding agreement on commissioned data processing with the processor.

(2) The cloud provider must ensure by means of appropriate TOMs that data are not processed until after a legally binding agreement on the commissioned data processing has been concluded with the processor.

(3) The legally binding agreement must be drafted in writing or an electronic form.

(4) The legally binding agreement on the commissioned data processing must meet the following requirements of this criterion, whereas the required definitions can may also be made in other documents if these have been included into the legally binding commissioned data processing agreement.

(5) The cloud provider must ensure that the object and duration of the processing are outlined as specifically as possible in the legally binding agreement on the commissioned data processing.

(6) The cloud provider must ensure that the legally binding agreement on the commissioned data processing determines the nature and purpose of the intended processing, the nature of data processed, and the categories of data subjects.

(7) The cloud provider must ensure that the legally binding agreement on the commissioned data processing determines that personal data will only be processed by the processor in accordance with documented instructions by the cloud provider, even as relates to the transfer of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor must inform the cloud provider of the legal requirement obligation before the processing, unless that law prohibits such information on important grounds of public interest. In this case, the legally binding agreement on the commissioned data processing contains the obligation of the processor to notify the cloud provider of these legal requirements before processing, unless that law in question prohibits such information on important grounds of public interest.

(8) In case the commissioned data processing includes the instruction-bound transfer of personal data to third countries or international organisations, the cloud provider must ensure that the legally binding agreement on the commissioned data processing determines the instruments according to Art. 45 GDPR or Art. 46 (2) and (3) GDPR, which are to be used for the transfers and, if applicable, also the other supplementary measures to be taken to ensure an appropriate level of protection.

(9) The cloud provider must ensure that the legally binding agreement on the commissioned data processing determines that the processor undertakes to inform the cloud provider if it believes that an instruction from the cloud provider infringes data protection regulations.

(10) The cloud provider must ensure that the legally binding agreement on the commissioned data processing determines the place of the data processing. If the data processing takes place outside the EU or the EEA, the specific third country must be stated.

(11) The cloud provider must ensure that the processor undertakes in the legally binding agreement on the commissioned data processing to notify the cloud provider without undue delay of any changes of the place of the data processing.

(12) The cloud provider must ensure that the legally binding agreement on the commissioned data processing determines that, before the start of the data processing operations, the processor commits the persons authorised to process personal data to confidentiality that continues to apply beyond the end of their employment relationship, unless they are already subject to a suitably comparable statutory obligation of confidentiality.

(13) The cloud provider must ensure that, in accordance with Art. 32 GDPR, the TOMs appropriate to the level of security of the outsourced data processing are determined in the legally binding agreement on the commissioned data processing.

(14) The cloud provider must ensure that the legally binding agreement on the commissioned data processing determines how the processor complies with the requirements in accordance with Art. 28 (2) and (4) GDPR for the use of the services of other processors.

(15) The obligations of the processor to return data media, return data and for unrecoverable erase data after the end of the data processing must be set out in the legally binding agreement on the commissioned data processing.

(16) The legally binding agreement on the commissioned data processing must include information on support for the cloud provider in fulfilling the rights of the data subject and in its notification obligation in the event of data breaches.

Explanation

Since the cloud provider is seeking certification of its data processing operations, it must ensure that data processing by a sub-processor also complies with the requirements of the General Data Protection Regulation. For this, the cloud provider must first conclude a legally binding agreement with the processor that includes the obligation requirements under Art. 28 (3) subpara. 1 sent. 2.

Implementation guidance

The implementation guidance under no. 1 apply analogously to the conclusion of a legally binding agreement with a sub-processor.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 5.4.1.2, 5.4.1.3, 6.10.2.4, 6.12, 7.2.6.

Determination methods

- Document review, particularly legal analysis

Determination activities

The evaluator should inspect the list of sub-processors used and carry out a sample check of agreements concluded. An evaluator examines the agreements with other sub-processors including the necessary information for the conformity assessment. For the respective sub-processors, existing documents of the TOM, the data security concept or certificates should be examined on a sample basis. Further relevant documents can be included in the review, including the template contract for commissioned processing with sub-processors, guidelines and instructions, further guarantees of the sub-processors, internal control areas of the cloud provider on sub-processing controls, the data protection concept or the risk assessment for subcontracting.

No. 20.2 – Ensuring proper processing

Criterion

(1) The cloud provider must ensure that the processor processes personal data exclusively on the cloud provider's documented instructions (Art. 28 (3) subpara. 1 sent. 2 lit. a) and h), Art. 29; 32 (4) GDPR).

(2) The cloud provider must ensure that the processor informs the cloud provider if, in its opinion, an instruction infringes data protection regulations (Art. 28 (3) subpara. 1 sent. 2 lit. h) in conjunction with Art. 29 GDPR).

(3) The cloud provider must ensure for outsourced processing that the processor guarantees the confidentiality, integrity, and availability of data and systems, the resilience of the systems, and the availability of

and access to data after a physical or technical incident. The processor must regularly check and, if necessary, adapt the implemented TOMs (Art. 24, 25, 28, 32, 35 in conjunction with Art. 5 (1) lit. f) and (2) GDPR).

(4) The cloud provider must ensure that the processor obligates its employees to commit themselves to confidentiality remaining valid beyond the end of their employment relationship before data processing begins, unless they are subject to a statutory obligation of confidentiality (Art. 28 (3) subpara. 1 sent. 2 lit. b) and h) GDPR).

(5) The cloud provider must ensure that the processor entrusts only employees, who have the necessary professional knowledge and who are trained in data protection and data security with the performance of processing operations (Art. 28 (3) subpara. 1 sent. 2 lit. e) and f) GDPR)

(6) The cloud provider must ensure that the processor informs the cloud provider if the place of the data processing changes (Art. 28 (3) subpara. 1 sent. 2 lit. a) and h) GDPR).

(7) The cloud provider must ensure that the processor deletes or returns all the data media provided to it and all personal data after the end of the performance of services relating to processing or upon instruction from the cloud provider, and that it unrecoverably deletes existing copies (Art. 28 (3) subpara. 1 sent. 2 lit. g) and h) GDPR).

(8) The cloud provider must ensure that the processor assists the cloud provider for the fulfilment of the rights of the data subjects and documents all instructions for exercising the data subject's rights (Art. 28 (3) subpara. 1 sent. 2 lit. e) and h) in conjunction with Chapter III GDPR).

(9) The cloud provider must ensure that the processor designates a DPO if it is legally obligated to do so (Art. 37 to 39 GDPR, Sec. 38 (1); (2) in conjunction with Sec. 6 (5) sent. 2 BDSG).

(10) The cloud provider must obligate the processor to maintain a record of processing activities if it is legally obligated to do so (Art. 30 (2) to (5) GDPR).

(11) The cloud provider must ensure that the processor notifies the cloud provider without undue delay after becoming aware of a personal data breach and its extent (Art. 33 (2) and Art. 28 (3) subpara. 1 sent. 2 lit. f) GDPR).

(12) The cloud provider must ensure that the processor complies with all requirements under the legally binding agreement on the commissioned data processing pursuant to No. 20.1 and fulfils all requirements under these criteria (Art. 24 (1) GDPR).

(13) The cloud provider must ensure that the processor ensures, if it also uses sub-processors, that the further sub-processors comply with the requirements set out in the criteria no. 10.1 to 10.5 in Chapter V.

(14) If the commissioned data processing provides for the instruction-bound transfer of personal data to third countries or international organisations or if the processor is subject to the law of a third country, which obligates it to disclose personal data to public authorities of the third country, although the data processing exclusively takes place in the EU or in the EEA, the cloud provider must ensure that the processor complies with criterion no. 11.1 from Chapter VI (Art. 46 in conjunction with Art. 42 (1) and 2; Art. 48 GDPR).

(15) The cloud provider must obligate the processor to appoint a representative in accordance with criterion no. 11.2 under Chapter VI if the processor is legally obligated to do so (Art. 27 in conjunction with Art. 3 (2) GDPR).

Explanation

If the cloud provider engages a processor for processing data to fulfil the contract for the provision of the cloud service, it must not only conclude a legally binding agreement to this effect, which fulfils the requirements under Art. 28 (3) subpara. 1 sent. 2 GDPR, but it must also ensure that the processor implements the measures set out in the legally binding agreement and fulfils its other obligations under the General Data Protection Regulation.

Implementation guidance

Reference is made to the implementation guidance in ISO/IEC 27701 no. 5.4.1.2, 5.4.1.3, 6.12, 7.2.6

Determination methods

- Document review
- Auditing

Determination activities

An evaluator examines existing documents of the sub-processors (e.g., code of conducts, certificates, legally binding agreements (in particular with regard to instructions by the cloud provider and obligations of the sub-processor),

service descriptions, data security concepts, other guarantees) from which the guarantee of compliance with the GDPR results. In addition, the evaluator examines documents on the selection (e.g., protocols on selection considerations and decisions) and the performance of cloud provider's checks (e.g., protocols on sub-processor checks). Protocols on the fulfilment of obligations as a result of the involvement of other processors should be examined.

The assessment can be supported by interviews with employees about controlling sub-processors (e.g., assessing their awareness of procedural steps and guarantees of sub-processors). An interview of employees on the involvement of sub-processors in supporting the cloud provider's duties as main processors can also be carried out as part of an audit (e.g., testing employees' awareness of procedural steps and contact persons of the sub-processors).

D. References

BSI C5	Cloud Computing Compliance Controls Catalogue, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html, status 20.11.2019
BSI TR-02102-1	Cryptographic Mechanisms: Recommendations and Key Lengths, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html, status 22.02.2019
BSI TR-02102-2	Cryptographic Mechanisms: Recommendations and Key Lengths. Part 2 – Use of Transport Layer Security (TLS), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html, status 22.02.2019
BSI TR-02102-3	Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.html, status 25.01.2018
BSI TR-02102-4	Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Secure Shell (SSH), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.html, status 25.01.2018
DIN EN 1627	Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification, status 2011
DIN 66398	Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information, status 2016
DIN 66399	Destruction of data carriers, status 2012
Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679	European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf
Guidelines 4/2019 on Article 25 Data Protection by Design and by Default	European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, adopted on 20 October 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
ISO/IEC 11770-2	IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques, status 2018
ISO/IEC 19941	Information technology — Cloud computing — Interoperability and portability, status 2017
ISO/IEC 21964-1	Information technology — Destruction of data carriers — Part 1: Principles and definitions, status 2018
ISO/IEC 24760-1	IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts, status 2019
ISO/IEC 24760-2	Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements, status 2015
ISO/IEC 24760-3	Information technology — Security techniques — A framework for identity management — Part 3: Practice, status 2016
ISO 25237	Health informatics — Pseudonymization, as of 2017
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls, status 2013
ISO/IEC 27018	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, status 2019
ISO/IEC 27040	Information technology — Security techniques — Storage security, status 2015
ISO/IEC 27701	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, status 2019
ISO/IEC 29101	Information technology — Security techniques — Privacy architecture framework, as of 2018

ISO/IEC 29134	Information technology — Security techniques — Guidelines for privacy impact assessment, as of 2017
ISO/IEC 29146	Information technology — Security techniques — A framework for access management, as of 2016
ISO 31000	Risk management – Guidelines, status 2018
IEC 31010	Risk management — Risk assessment techniques, status 2019
SDM	Standard-Datenschutzmodell (Standard Data Protection Model), Version 2.0, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf, status 2019
Working paper „Requirements for the use of pseudonymisation solutions in compliance with data protection regulations"	Schwartmann/Weiß (ed.), Requirements for the use of pseudonymisation solutions in compliance with data protection regulations, a working paper of the Data Protection Focus Group of the Platform Security, Protection and Trust for Society and Business at the Digital Summit 2018, https://www.gdd.de/downloads/requirements-for-the-use-of-pseudonymisation-solutions
Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data	European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
Recommendations 02/2020 on the European Essential Guarantees for surveillance measures	European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.