European Cloud Service
Data Protection Certification

AUDITOR Criteria Catalogue

- Draft version 0.9 -

As of 28.03.2019

Related AUDITOR publications:

- object of certification
- concept of protection categories
- DIN SPEC 27557

Online available: www.auditor-cert.eu

Recommended Citation:

Roßnagel, A., Sunyaev, A., Lins, S., Maier, N., & Teigeler, H. (2019). AUDITOR Criteria Catalogue – Draft version 0.9. Karlsruhe, Germany: KIT. DOI: 10.5445/IR/1000092729

Online available: www.auditor-cert.eu

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

Authors

Alexander Roßnagel[a], Ali Sunyaev[b], Sebastian Lins[b], Natalie Maier[a], Heiner Teigeler[b]

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

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

Disclaimer

Please note that the AUDITOR consortium publishes all project-related findings initially in German and then translates them into English. Consequently, this document might contain linguistic or wording errors, for example, concerning the form for the expression of provisions (i.e., using shall, should, must, may and can). The AUDITOR consortium tries to continuously improve all documents to achieve a high level of maturity. If you identified any errors or have any concerns, please do not hesitate to contact the AUDITOR consortium (info@auditor-cert.eu).

Table of contents

List of abbreviations

Alt.	Alternative
Art.	Article
BDSG	Federal Data Protection Act (applicable as of 25.05.18)
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
TOM	Technical and organisational measures

Note on the gender-neutral wording:

All personal descriptions in the AUDITOR criteria catalogue are to be considered gender-neutral. Therefore, for the purpose of improved readability, there is no gender-specific wording, with the result that any grammatically masculine forms are to be considered contextually neutral (e.g., in the name of “data protection officer”, the functional description is to be read as neutral and does not specifically reference a male).

A. Object and objectives of the AUDITOR Criteria Catalogue

The AUDITOR criteria catalogue is a testing standard for the data protection certification of cloud services in accordance with the requirements of the EU General Data Protection Regulation (GDPR).

1. Addressees and function of the AUDITOR Criteria Catalogue

AUDITOR data protection certification enables providers of cloud services in the private sector to demonstrate the compatibility of their data processing operations with legal data protection requirements. The AUDITOR criteria catalogue describes the legal data protection requirements for the processing of personal data on the part of the contractor (cloud provider). However, the legal data protection requirements of the clients (cloud users) are not addressed.

AUDITOR object of certification

The certification object of the AUDITOR mechanism are operations of processing personal data in the context of cloud services. According to Art. 4 No. 2 GDPR data processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. This includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

The certification covers data processing operations that are provided in products or services, or with the assistance of products and services (including more than one). The AUDITOR mechanism considers the data processing operations that the cloud provider performs as a processor in the context of order processing in accordance with Art. 28 GDPR. Furthermore, data processing operations are considered which the cloud provider undertakes in order to conclude and execute the contract with the cloud user about the provision of the cloud service and to fulfil legal obligations.

When determining the object of certification, there are three components that cloud providers must consider to as an addressee of the AUDITOR certification mechanism: 1. personal data; 2. technical systems (infrastructure, hardware and software used to process the personal data) and 3. processes and procedures related to the processing operations. Thus, a data processing operation usually consists of both technical and automated as well as non-technical organisational components which process personal data for a specific purpose and whose data protection measures are taken into account in data protection concepts and combined into data protection management systems. The entire data processing operation must comply with the requirements of the General Data Protection Regulation.

Data processing operations must have a self-contained procedural structure for the processing of personal data, within which the specific data protection risks of the respective cloud service can be completely considered. This means that interfaces of the certified cloud services with other services must also be considered, in order to identify data flows from which data protection risks may arise. Further information about the AUDITOR object of certification can be found in the accompanying ″object of certification" document.

Cloud providers as the addressees

A *cloud provider* within the meaning of this catalogue is any company in the private sector that provides a cloud service in the market and would like to be certified in accordance with the AUDITOR criteria catalogue as a processor in accordance with Art. 4 No. 8 GDPR.

Cloud providers are the applicants in the AUDITOR certification mechanism and are addressed by the AUDITOR criteria catalogue in two ways:

1) *As the processor* of data processing operations. Cloud providers can be both B2B and B2C providers. What is important is that they are the processor of the data that is processed in the cloud (“**content or application data**”) and not the controller and would like to have the data protection conformity of their data processing operations confirmed by a certificate. For B2B in particular, the content and application Data will often be personal data of customers, employees, or other data subjects with whom the cloud user has a contractual relationship. However, content and application data may also be personal data of the cloud user.

2) *As the controller* of data processing operations. The cloud provider will also be addressed as the controller of data processing operations that are necessary to enter into and perform the contract on the provision of the cloud service with the cloud user. These data processing operations concern the protection of the cloud user's personal data and personal privacy. Third-party personal data such as of customers or employees of the cloud user is handled as part of the processing agreed between the cloud user and the cloud provider and only obligates the cloud provider in its role as processor. Where the cloud user concludes a contract with the cloud provider on the provision and use of cloud services, the cloud provider will be obligated to process personal data above all through recording and retention obligations under commercial and tax law so that data processing for the fulfilment of legal obligations also falls within the scope of the AUDITOR certification.

   Although the cloud provider is free to choose the processing purpose, and the appropriate legal basis thereto under Art. 6 para. 1 subpara. 1 lit. a-f GDPR and Art. 5 para. 1 lit. b in connection with Art. 6 para. 4 GDPR does not have a strict purpose limitation but knows only an agreement for a specific purpose, only the data processing of the cloud provider in its role as the controller will be considered for the AUDITOR certification that is intrinsically linked to the contract between the cloud provider and the cloud user for the provision and use of the cloud service and the performance of the data processing. As part of the AUDITOR certification, only those data processing operations are considered that the cloud provider performs in order to provide the cloud service to the cloud user so as to enable the use of the service and to invoice the user accordingly.

   In order to conclude and execute the contract with the cloud user on the use of the cloud service, the cloud provider shall decide which personal data it collects and processes. As a rule, data such as names, addresses, payment information such as bank account information, phone numbers, user names, and passwords for logging into the cloud service is processed. They can be grouped under the term **"personal information"**.

   In order to enable the cloud user to make use of the cloud service and to invoice the user accordingly, the cloud provider must process additional personal data such as login/logout data for user accounts, IP addresses, the used service modules, and the extent of use. This data can be grouped under the term **"usage data"**.

   Because the General Data Protection Regulation does not differentiate between personal information and usage data, for this criteria catalogue, this data is referred to as **personal data**, which is made available when performing the contract for the provision of cloud services.

Cloud users as beneficiaries

A *cloud* user within the meaning of this catalogue is any natural or legal person who carries out the processing of personal data as a controller in accordance with Art. 4 No. 7 GDPR and determines alone or jointly with others about the purposes and means of this processing and decides to outsource this processing to a cloud provider.

On the basis of the certification of the data processing operations of a cloud service, the cloud user can trust that the cloud service it uses is data protection compliant. The scope of applicability of the data protection certification in accordance with AUDITOR is the processing of personal data by order (processing) in accordance with Art. 28 GDPR by a cloud provider. In this case, the cloud user of the service, as a client, must in accordance with Art. 28 para. 1 GDPR be satisfied that there are sufficient guarantees provided by the cloud provider to confirm that appropriate technical and organisational measures (TOM) are implemented in such a manner that the processing will meet the requirements of the General Data Protection Regulation, and to ensure the protection of the rights of the data subject. The demonstration of sufficient guarantees is made easier if the cloud provider, as the contractor, presents a certificate that confirms the fulfilment of the legal requirements, as a certificate may be used in accordance with Art. 28 para. 5 GDPR as an element to demonstrate sufficient guarantees. For the use of cloud services that are, as a rule, provided as standardised services for a variety of users, the data protection certification is particularly important because it represents an efficient way of fulfilling the statutory verification obligation.

Personal data as goods to be protected

Personal data in accordance with the legal definition under Art. 4 para 1 GDPR are all data that relate to an identified or identifiable natural person. In a cloud context, this could be, for instance, application

data of the cloud user, if it enables the respective data processor to identify a natural person or make a natural person identifiable. In accordance with Art. 28 para. 3 sentence 1 GDPR, the cloud users and cloud providers must set, in a legally binding data processing agreement, which types of personal data are to be processed by the processor, bound by instruction, within the framework of the processing on the behalf of the controller.

Dividing up responsibilities between the cloud provider and the cloud user

Because the scope of the data protection certification pursuant to AUDITOR includes the processing of personal data on the behalf of the controller under Art. 28 GDPR, the AUDITOR criteria catalogue focuses on the legal data protection requirements for the cloud provider in its role as a processor. Data processing operations for which the cloud provider does not merely act under authority but, as the controller, decides on the purpose and means of processing personal data, are only considered in the context of the AUDITOR certification insofar as data processing operations are involved that are necessary in order to conclude and execute the contract with the cloud user for the provision of the cloud service and to be able to fulfil legal obligations, such as commercial and fiscal recording and retention obligations.

It is not uncommon that cloud computing regularly leads to a coexistence of responsibilities between the cloud provider and the cloud user. General guidelines on the division of responsibility are difficult to formulate since the distribution of responsibilities largely depends on the service models and the specific designs as well as the individual processing agreements with the cloud users. It is therefore up to the cloud user and cloud provider to determine rules for distributing responsibilities.

The regulations must reflect the intentions and objectives of the parties. When it comes to the relationship between the cloud user and the cloud provider, the cloud provider is always the contractor where it does not pursue its own purposes with the data to be processed, even if it makes decisions about the means of data processing. The cloud provider is only the controller if it pursues its own purposes with the data. The cloud provider will remain the processor, however, when the cloud user clearly defines the processing purpose but leaves the decision-making power as regards the choice of technical and organisational means to the cloud provider, insofar as such means are suitable for achieving the purposes of the processing, and the cloud provider informs the cloud user thereof.

As a rule of thumb, the cloud user should regularly be regarded as the controller for the personal data that it, or persons associated with the user, transfers into the cloud. This concerns the cloud user's content and application data. The cloud provider is responsible for those data processing operations that it undertakes to perform the cloud service and to enable its use and to invoice the user accordingly. As a rule, this concerns personal information and usage data in the cloud.

Dividing up responsibilities between the cloud provider and the sub-processor

The cloud provider has the opportunity not to provide the full cloud service itself, but to use other sub-processors for the provision of services, as long as the cloud user agrees to that. In this case, individual sections or parts of the data processing can be delegated or outsourced to other processors, resulting in a service chain. However, the outsourcing of the data processing to other sub-processors may not have the result, that the provisions of the General Data Protection Regulation are being ignored in the service chain. Instead, the cloud provider must ensure, as the main processor, that the relevant provisions of the General Data Protection Regulation are observed by all sub-processors at all levels. The cloud provider remains universally responsible for the execution of the instructions for the cloud user.

If the processing operations of a cloud service to be certified are based on platforms or infrastructures not owned by the provider or if the processor uses other sub-processors, the certificate may only refer to those data processing operations that are the responsibility of the respective processor. However, the processor must be convinced that these third-party platforms, infrastructures and sub-processors used by it also comply with the data protection regulations relevant to them and may only use them to provide its service. A cloud provider may therefore only select those sub-processors which, in accordance with Article 28 para. 1 GDPR, provide "*sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*" Sub-processors can, for their part, provide the required suitable guarantees, e.g. by means of a data protection certificate or by following approved codes of conduct pursuant to Art. 40 GDPR. Chapter V of this criteria catalogue regulates sub-processing in particular.

2. TCDP development pursuant to the General Data Protection Regulation

The certification in accordance with the old German Federal Data Protection Act was examined in the pilot project "Data Protection Certification for Cloud Services" by the Trusted Cloud Data Protection Profile (TCDP), that was finalised in September 2016. Since not all relevant international standards, newly developed relevant sets of criteria – e.g. Cloud Computing Compliance Controls Catalogue – and in particular the requirements of the basic data protection regulation could be taken into account when developing the certification criteria according to TCDP, the TCDP set of criteria must be adapted to the new regulations with the application of the General Data Protection Regulation on 25 May 2018. This takes place with the AUDITOR criteria catalogue. This is aimed in particular at uniform criteria for union-wide certification.

The AUDITOR criteria catalogue focuses all relevant provisions for the data protection certification of cloud services in the General Data Protection Regulation, and specifies them to create testable criteria.

B. Structure and use of the AUDITOR Criteria Catalogue

1. Elements of the AUDITOR Criteria Catalogue

The AUDITOR criteria catalogue contains "criteria", "explanations", “implementation guidance” and “demonstrating compliance”. The "criteria" describe the normative requirements that must be fulfilled in order to receive a certificate on the basis of the AUDITOR criteria catalogue. They therefore represent the requirements that an accredited certification body examines as part of the certification mechanism. The "explanations" are intended to make the understanding of the criteria and their derivation from the law easier.

For each criterion, “implementation guidance” serves as guidelines using typical examples for understanding and implementing the criteria; however, they are not binding. Moreover, there is a “*demonstrating compliance*” part for each criterion. The “*demonstrating compliance*” part provides the answer to the question of how the existence of the criteria can be proven in the specific certification mechanism. Similar to the implementation guidance, this part serves as a guideline and provides assistance 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. The accredited AUDITOR conformity assessment programme determines how each criterion should be verified for the certification.

The criteria catalogue differentiates between criteria, explanations, implementation guidance, and demonstrating compliance for processing application data (Chapter C) and for processing personal information and usage data for which a cloud provider is responsible (Chapter D).

2. Protection categories

Requirements for TOM of the cloud service are differentiated in accordance with protection categories. The AUDITOR criteria catalogue is thereby orientated to the TCDP protection categories concept, but also considers the protection requirement grading in accordance with the Standard Data Protection Model or Standard-Datenschutzmodell (SDM) of the German data protection supervisory authorities.

2.1 The concept of protection categories

The concept of protection categories is based on the risk of data processing for the fundamental rights and freedoms of natural persons. In addition, in accordance with Art. 24, 25 and 32 GDPR, the selection of TOM must also consider the state of the art and implementation costs. Taking into account Recital 75, 76, 85, 90, 91, 94, 95 and 96, the controller must identify each risk to the rights and freedoms of natural persons in advance when processing personal data. In another step, it must be assessed whether the processing could lead to material or immaterial damage, particularly if it could lead to discrimination, identity theft or fraud, financial loss, damage to reputation, a loss of confidentiality of the personal data protected by professional secrecy, an unauthorised reversal of pseudonymity, or other significant economic or social disadvantages, if the data subject is deprived of its rights and freedoms, or prevented from controlling its personal data.

In accordance with Recital 76 sentence 1, the controller must determine the likelihood and severity of the risk to the rights and freedoms of the data subject by reference to the nature, scope, context and purposes of the processing. The controller should assess this risk in accordance with the respective utilisation context of the processed personal data on the basis of an objective assessment. It must thereby determine, in accordance with Recital 76 sentence 2, whether the data processing involves a risk or a high risk. These risk classifications are implemented with the AUDITOR concept of protection categories.

Conversely, the cloud provider must signify, with its service description, for which type and categories of data and for which protection category the service offered is suitable. Each tested data processing operation in this cloud service must therefore comply with this protection category. Protection categories are therefore not allocated to each individual data protection operation, but the cloud service as such.

The objective of the concept of protection categories is to simplify the individual benchmark of the General Data Protection Regulation – the TOM requirements are based on the required protection need for

the respective data processing – by allocation to protection categories. The protection categories therefore have a dual function: they describe the required protection needs for the data processing operations as well as the TOM requirements. In order to make the different functions clear, the concept of protection categories distinguishes between the categories of protection needs and the categories of protection requirements.

The categories of protection needs define the protection needs for data protection operations on the basis of general characteristics. This is derived from the nature of data, the scope, the context, and the purposes of the specific data processing.

The categories of protection requirements define, in a general manner, the technical and organisational requirements that are significant for the data processing services of the categories concerned. A corresponding category of protection requirements is thereby defined for each category of protection needs.

The differentiation of categories of protection needs and protection requirements corresponds with the roles and responsibilities of cloud users as controllers and cloud providers as processors. Within the framework of the certification process, the cloud provider claims a specific category of protection requirements for each service based on the evaluation and by means of the specific TOM. This is reviewed by the certification body. The suitability of the cloud service for a specific category of protection requirements is expressed in the certificate. As a controller and contractee, however, the cloud user has the task of determining the required protection needs for its data processing, by selecting a category of protection needs. If it outsources its data processing to a cloud service, it must select a cloud service that at least fulfils the respective category of protection requirements.

With respect to the data processing for which the cloud provider is responsible and which is necessary to perform the cloud service for use by the cloud user, the provider shall determine both the protection need and the protection requirements of the data processing as both are the provider's responsibility.

2.2 The protection categories of the AUDITOR Criteria Catalogue

The AUDITOR criteria catalogue is based on the differentiation of three protection categories (I, II, III), for which the respective protection needs (categories of protection needs) and protection requirements (categories of protection requirement) are described.

In addition to the three protection categories, there are data processing operations that do not provide – nor generate, assist, or enable – an indication of personal or factual affairs of natural persons and, therefore, do not have any protection needs under data protection laws. They are below protection category 1, which is why they are not considered in the Concept of Protection Categories.

Data processing operations with an extremely high protection need (above category of protection needs 3) are also not considered in the Concept of Protection Categories and the AUDITOR certification. There is an extremely high need for protection when, on the basis of the data used or the actual processing of such data, the data processing operations have, can support, or lead to a critical informative value concerning the personality or circumstances of the data subject or are otherwise of considerable importance for the circumstances of the data subject, and when the unauthorised processing of such data would lead to a concrete risk of substantial impairment of the life, health, or freedom of the data subject.

Non-exhaustive examples of data with extremely high protection needs:

- Data from undercover informants of the Federal Office for the Protection of the Constitution;
- Data on persons who may be potential victims of criminal offences;
- Addresses of witnesses in specific criminal proceedings.

Data processing operations with individually strongly diverging circumstances are also not considered in the Concept of Protection Categories and the AUDITOR certification because they are not accessible to the generalization associated with the Concept of Protection Categories.

a) Ascertaining the category of protection needs

It is up to the cloud user to determine the protection needs. The protection needs are ascertained in a three-step process:

- In step 1, the abstract protection needs of the data to be processed are determined based on the data type.

- In step 2, it must be checked whether the protection needs are increased due to the specific use of the data.
- In step 3, it must be checked whether the protection needs decrease due to specific circumstances.

As a result, the protection needs of the specific data processing are categorised in accordance with the categories of protection needs. Steps two and three are not explained any further in the AUDITOR catalogue, because they concern the cloud user and not the certification of the cloud provider as such.

It should be noted that the cloud provider is the controller for the data processing as part of performing the contact with the cloud user, and the cloud provider must therefore also determine the protection need of this data processing.

Categories of protection needs according to data type (abstract protection needs – step 1)

Then, the abstract protection need of the data to be processed is determined according to the data type. This forms the starting point and is only for the initial sorting of the data. Ultimately, the protection need of data cannot be determined in an abstract manner, but rather depends on its respective usage context.

Data types with a normal protection need (category of protection needs 1)

All processing of personal data constitutes an infringement of the fundamental rights of the data subject. For this reason, it is assumed that all processing of personal data includes at least a normal protection need.

Category of protection needs 1 includes all data processing operations that, due to the data entered and the specific processing of this data, contain, generate, assist or enable statements about the personal or factual affairs of the data subject. The unauthorised use of this data can easily be prevented or ceased by the data subject through taking action or does not result in any specific impairments for the data subject.

Non-exhaustive examples of data (without a processing context, as long as not in category of protection needs 2 or 3):

- Name;
- Gender;
- Address;
- Profession;
- Year of birth;
- Title;
- Address book information;
- Telephone records;
- Nationality;
- Telephone number of a natural person.

Data types with a high protection need (category of needs 2)

Data processing operations that, due to the data used or the specific processing of these data are capable of providing or sustaining informative value about the personality or the life of the data subject or that could lead to such information or that are otherwise of significance to the data subject's affairs. The unauthorised processing of such data may lead to impairments to the social status or economic circumstances of the data subject ("reputation"). In addition, data that were identified as particularly worthy of protection by the legislator in Art. 9 para. 1 GDPR must be presumed to have a high protection need.

Non-exhaustive examples of data (without a processing context, as long as not in category of protection needs 3):

- Name, address of a contracting party;
- Date of birth;
- Marital status;
- Family relations and acquaintanceships;
- Data on business and contractual relationships;
- Context on a contractual partner (e.g., subject-matter of an agreed service);

- Processing of non-changeable personal data that can serve as a lifelong anchor for profiling, such as genetic data within the meaning of Art. 4 No. 13 GDPR, or biometric data within the meaning of Art. 4 No. 14 GDPR;
- Data on racial and ethnic origin;
- Data on political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Data about the sex life or sexual orientation of a natural person;
- Processing of clearly identifiable, highly linkable data such as health insurance numbers or tax numbers;
- Data that have potential effects on the standing/reputation of a data subject;
- Data about the protected inner life of the data subject (e.g., diaries)
- Data concerning health within the meaning of Art. 4 No. 15 GDPR;
- Degree of disability;
- Processing of data with inherent lack of transparency for the data subject (estimated values for scoring, application of algorithms);
- Income;
- Social benefits;
- Taxes;
- Administrative offences;
- Data on rental agreements;
- Patient administration data (with the exception of particularly sensitive diagnostic data and the like);
- Work time data;
- Membership directories;
- Civil register;
- Certificates and exam results;
- Insurance data;
- Personnel administration data from employment relationships (with the exception of company assessments and professional career);
- Traffic offences;
- Simple evaluations of little importance (e.g., yes/no decision for classification in a mobile phone contract, etc.,);
- Access data for a service;
- Content of communication with a person (e.g., email content data, letter, telephone call);
- (Exact) location of a person;
- Financial data about a person (e.g., account balance, credit card number, individual payment);
- Credit reports;
- Telecommunications traffic data.

Explanatory note: Communication contents, especially written or audio recordings of all types, can have very different protection needs, from low to very high. Determining the protection need requires an objective assessment in which the extent of the risk of the data processing is evaluated. If the cloud user has no knowledge of the subjective protection need of the communicating party (e.g., general collaboration service with data storage, video conference and mail function) or offers its services for communication that is particularly worthy of protection (e.g., conference services for lawyers and clients, here: protection category 3), it may assume the category of protection needs 2.

Data types with a very high protection need (category of protection needs 3)

Data processing operations that, due to the data used or the specific processing of these data are capable of providing or sustaining considerable informative value about the personality or the life of the data subject, or that could lead to such information or that are otherwise of considerable significance to the data subject's affairs. The unauthorised processing of such data may lead to considerable disadvantages for the data subject regarding its social status and its economic circumstances ("livelihood").

Explanatory note: Data types in this sense also include data majorities, in particular linked data (e.g., personality profiles) that result in new information content.

Non-exhaustive examples of data with very high protection needs:

- Data subject to professional, business, telecommunications or client secrecy (e.g., patient data, client data);
- Data of which the knowledge enables significant specific harm to the data subject or third party (e.g., personal identification number, transaction number in online banking);
- Debts;
- Particularly sensitive social data;
- Seizures;
- Personnel administration data such as company assessments, professional career and the like, as long as not in category of protection needs 2;
- Data about previous convictions and circumstances related to criminal proceedings (e.g., preliminary proceedings) of a person and corresponding suspicions, delinquencies;
- Particularly sensitive data concerning health within the meaning of Art 4 No. 15 GDPR, such as data about illnesses, the knowledge of which is unpleasant to the data subject to a particular extent, or which could lead to social stigmatisation of the data subject;
- Personality profiles, e.g., movement profile, relationship profile, interest profile, purchase behaviour profile, with considerable informative value about the personality of the data subject.

b) Categories of protection requirements

The categories of protection requirements serve to define the TOMs that are appropriate to adequately protect the rights and freedoms of data subjects in relation to the risks of service identified in the category of protection needs.

Category of protection requirements 1

By taking risk-appropriate TOMs, the cloud provider must ensure data minimisation, availability, integrity, confidentiality, unlinkability, transparency, and intervenability of personal data (see protection goals under the Standard Data Protection Model). For information security, this means that data must be protected against destruction, loss, alteration, unauthorised access, and disclosure in particular, and the resilience of the cloud service must be guaranteed.

As a rule, the TOMs must be appropriate for excluding such processes due to technical or organisational errors, including operating errors, of the cloud provider or its employees or due to acts of negligence of third parties. A minimum level of protection must be provided to make intentional interferences more difficult to achieve. It must be possible to determine each interference at a later date.

Category of protection requirements 2

A high protection need leads to additional or more effective risk-appropriate TOMs having to be taken in order to ensure data minimisation, availability, integrity, confidentiality, unlinkability, transparency, and intervenability of personal data (see protection goals under the Standard Data Protection Model, or Standard-Datenschutzmodell, SDM). For information security, this means that data must be protected against destruction, loss, alteration, unauthorised access, and disclosure in particular, and the resilience of the cloud service must be guaranteed. At the same time, the measures appropriate for category of protection requirements 1 must be fulfilled and their design adapted to the protection need.

This can be achieved by increasing the effect of a measure insofar as it provides a starting point for such scaling. An example of this is increasing the length of the used cryptographic keys or using hardware tokens or two-factor authentication. Furthermore, an adjustment can be made by ensuring that the measure is carried out with greater reliability in accordance with the specifications. For this, possible disturbance influences must be determined and the robustness of the measures must be increased by taking additional precautions, which are often organisational ones.

As a rule, the measures taken must be appropriate for excluding such processes due to technical or organisational errors, including operating errors, of the cloud provider or its employees or due to acts of negligence of third parties. As a rule, the measures must also be appropriate for preventing damage caused by negligent actions of authorised persons. Protection must be provided that rules out expected interference with sufficient certainty. This includes adequate protection against known attack scenarios in particular as well as measures through which interferences can normally be detected (subsequently).

Category of protection requirements 3

In addition to the TOMs of the categories of protection requirements 1 and 2, the cloud provider must achieve risk-appropriate TOMs to protect the data, in particular against destruction, loss, alteration, unauthorised access, and unauthorised disclosure.

The measures must be appropriate for excluding with sufficient certainty such processes due to technical or organisational errors, including operating errors, or due to acts of negligence or intent. This includes sufficient protection against known attack scenarios in particular as well as procedures for identifying abuse. It must be possible to determine each interference at a later date.

3. Inapplicability of criteria

As part of the certification mechanisms, the cloud provider will provide the certification body with sufficient information for assessing, defining, and finalising the object of the certification. This includes in particular documenting responsibilities and, insofar as is applicable, involving sub-processors in the data processing operations to be certified. When specifying the object of the certification or during the audit process, the certification body can determine whether individual criteria are not applicable to the data processing operation under consideration. The accredited AUDITOR conformity assessment programme regulates the requirements and the procedure for determining and assessing the inapplicability of criteria. It is thus required that non-applicable criteria be identified on the certificate.

Criteria are not applicable, in particular, if the cloud provider cannot perform them because they are outside its area of responsibility. For example, the cloud provider is thus obligated to assist the cloud user in providing information according to the criterion No. 6.1. However, the criterion does not apply to the cloud provider's data processing operations, therefore exempting the cloud provider from providing information if the cloud user is responsible for the data in question and makes decisions concerning applications and files. The same applies when not the cloud provider but the sub-processor is responsible for access to data processing systems pursuant to No. 2.3. In this case, criterion No. 2.3 is not applicable for the cloud provider. The cloud provider must, however, be convinced that the sub-processors comply with the data protection regulations relevant to them (see No. 10.4), thereby in turn fulfilling criterion No. 2.3.

Furthermore, criteria are not applicable when the cloud provider does not perform the tasks described in the criteria. If the cloud provider does not, for example, utilise sub-processors or if no data is processed outside of the European Union or the European Economic Area, the criteria in Chapters V and VI are not applicable.

C. Criteria and implementation recommendations for order processing

Chapter I: Legally binding order 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] that fulfils the legal requirements for order 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, which apply independent of the cloud service's respective service model.

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

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

Criterion

(1) The cloud provider ensures, with appropriate technical or organisational precautions, that the cloud service is only provided after the conclusion of a legally binding order processing agreement with the cloud user.

(2) This agreement must meet the criteria of this chapter (No. 1.1 to 1.8).

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

Explanation

The legally binding agreement on processing by order is essential, because it explicitly clarifies the role of the cloud provider as a processor within the meaning of Art. 4 No. 8 GDPR in comparison to the role of the cloud user as a controller. This agreement is often based on another service provision agreement; both agreements must be differentiated.

Implementation guidance

The cloud provider shall make technical or organisational precautions to ensure an automatic conclusion of the agreement before the service is actually used. The potential cloud user may thus be notified of an agreement relating thereto during registration, which it must confirm before using the service.

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

Demonstrating compliance

As part of the certification, the cloud provider can provide all or a representative sample of legally binding agreements that it concludes with the cloud user. The cloud provider can further demonstrate compliance by means of appropriate documentation showing that technical or organisational precautions were taken to ensure that the service can be used only after the agreement has been concluded.

[1] Art. 28 para. 3 sentence 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 within the meaning of Art. 28 para. 3 sentence 1 GDPR may apply as the legal basis for the processing.

[2] For the electronic form, text form within the meaning of Sec. 126b BGB (German Civil Code) suffices.

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

Criterion

(1) The subject-matter and the duration of the processing must be outlined as specifically as possible in the legally binding agreement on the order processing.

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

(3) The conditions for termination must be laid down in the agreement.

Implementation guidance

Restricting the subject-matter of the contract in such a way should make it clear to both parties which processing operations or categories are carried out by the cloud provider for the cloud user. The influence the cloud provider has on choosing the processing means to carry out processing operations involving personal data should be set out in a transparent manner. Regulations on the processing subject-matter should also reflect the clearly defined areas of responsibility between cloud users and cloud providers.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by showing a draft of a legally binding agreement containing such information and by implementing a procedure after which the agreement is entered into with those specifications.

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

Criterion

In the legally binding agreement on the order processing, 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, must be determined.

Implementation guidance

Although this information does not have to cover every specific individual case, they should be sufficiently precise so that the data processing operations permitted under the contract can be followed in detail from the point of view of the cloud user.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by showing a draft of a legally binding agreement containing such information and by implementing a procedure after which the agreement is entered into with those specifications.

No. 1.4 – Determination of authority of the cloud user (Art. 28 para. 3 sentence 2 lit. a GDPR)

Criterion

(1) The legally binding data processing agreement provides that the personal data will only be processed upon documented instruction by the controller – even in relation to the transfer of personal data to a third country or an international organisation.

(2) If no individual legally binding agreement is entered into within the framework of standardised bulk transactions, the cloud provider must name, as precisely as possible, the services it can technically perform in a manner traceable from a cloud user perspective in its service description, in order to enable a selection in accordance with Art. 28 para. 1 GDPR.

Explanation

The dependence on instructions is named at multiple points in the General Data Protection Regulation (Art. 28 para. 3 sentence 2 lit. a; Art. 28 para. 3 sentence 3 GDPR, indirectly in Art. 28 para. 10 and Art. 29, Art. 32 para. 4 GDPR).

If the cloud provider exceeds the limits of the cloud user in accordance with its instructions, there is a violation in accordance with Art. 28 para. 10 and Art. 29 GDPR, and the cloud provider must expect liability consequences.

Implementation guidance

The legally binding 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 may be specified in the legally binding data processing agreement and their means of authentication may be specified.

In the legally binding data processing agreement or in standard clauses of the cloud provider, the technically feasible services and the cloud user's authorities to issue instruction must be listed. The legally binding agreement should set out the options available to the cloud user to exercise its authority. In particular they can exist in automated procedures. 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 para.1 GDPR. Where this is the case, the cloud user, by selecting the cloud service, will instruct the cloud provider to perform the described, standardised service.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by disclosing the corresponding regulations on issuing instructions in the legally binding agreements and by presenting existing documentation of individual authoritative instructions.

No. 1.5 – place of data processing (indirectly in Art. 28 para. 3 sentence 2 lit. a GDPR)

Criterion

(1) In the legally binding data processing agreement, it is 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 determines that in the event that the place of processing changes during its period of validity for reasons which are the responsibility of the cloud provider or unforeseeable for both parties, the cloud provider shall notify the cloud user immediately of such a change.

(4) In the event of any significant deviation from the set place of the data processing, the cloud user is granted an immediate right of termination from the legally binding agreement.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by showing a draft of a legally binding agreement in which it undertakes to inform the cloud user immediately of any changes to the place of data processing.

No. 1.6 – Confidentiality obligation (Art. 28 para. 3 sentence 2 lit. b GDPR)

Criterion

The cloud provider is obliged, in the legally binding data processing agreement, to commit the persons authorised to process personal data to confidentiality before the start of the data processing activity, unless they are already subject to a suitably comparable statutory obligation of confidentiality.

Explanation

The confidentiality obligation and secrecy instruction promote the protection goal of confidentiality (SDM 6.2.3)

Demonstrating compliance

The cloud provider can demonstrate compliance by keeping a draft of a legally binding agreement in which the cloud provider commits that persons authorised to process the personal data have committed themselves to confidentiality before starting data processing activities, unless they are already subject to a suitably comparable statutory obligation of confidentiality.

No. 1.7 – Technical and organisational measures, subcontracting and assistance (Art. 28 para. 3 sentence 2 lit. c–f in connection with Chap. III and Art. 32–36 GDPR)

Criterion

(1) The protection category and the TOM to be taken are laid down in a legally binding data processing agreement.

(2) The legally binding data processing agreement includes 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. The maximum number of people from the staff of the cloud provider and its sub-processors, for which the pseudonymisation or encryption is not applicable, must be stated.

(3) In the legally binding data processing agreement, the cloud provider shall lay down at what level and how quickly (within what time frame) after a physical or technical incident it can restore the cloud user's data and the cloud service and guarantee the cloud user access to the cloud service and the data (No. 2.11).

(4) In the legally binding data processing agreement, it is determined how the cloud provider complies with the requirements in accordance with Art. 28 para. 2 and 4 GDPR for the use of the services of other processors.

(5) The procedures to assist the cloud user when satisfying the rights of the data subject in accordance with No. 6, when carrying out a data protection impact assessment in accordance with No. 7, and when fulfilling the reporting obligation in the event of data protection breaches in accordance with No. 8.2, are laid down in the legally binding 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 to which category of protection requirements the cloud service corresponds.

The requirements of Art. 28 para. 3 sentence 2 lit. d GDPR should be specified in the legally binding data processing agreement so that compliance can be easily verified by the cloud user.

Since the cloud user has a right of object against changes in sub-processing (No. 10.3), the legally binding 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 data processing agreement should specify the cloud provider's assistance 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.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by showing a draft of a legally binding agreement containing such information and by implementing a procedure after which the agreement is entered into with those specifications.

No. 1.8 – Return of data media and erasure of data (Art. 28 para. 3 sentence 2 lit. g GDPR)

Criterion

The obligations of the cloud provider to return data media, return data and erase data after the end of the data processing must be set out in a legally binding order processing agreement.

Explanation

If the cloud provider is obliged to store or keep data due to legal obligations even after the end of the order processing, these data are not to be deleted. This should be noted accordingly in the legally binding order processing agreement.

Implementation guidance

Compliance with the requirements of having returned data media and having deleted data can also be demonstrated by referencing the corresponding principles of the cloud provider. The cloud user can choose how this is executed. The cloud provider's obligations are waived if it has a storage obligation in accordance with Union law or the law of the Member States.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by showing a draft of a legally binding agreement containing such specifications and by having implemented a procedure after which the agreement is concluded with those specifications.

Chapter II: Rights and obligations of the cloud provider

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

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

Criterion

(1) The cloud provider shall conduct a risk analysis with regard to data security and shall have a data security concept that corresponds to its protection category and is appropriate for the specific risks of its data processing operations.

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

(3) The data security concept shall be documented in writing.

(4) The data security concept shall be reviewed at regular intervals to ensure that it is up to date and appropriate and shall be updated as necessary.

(5) The data security concept describes which data processing operations are the cloud provider's responsibility and for which data processing operations involved sub-processors are responsible.

(6) The data security concept describes which data processing operations are the cloud provider's responsibility and which are the cloud user's.

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

Explanation

The cloud provider must set risk-appropriate TOM 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 thereby concerned must be discernible 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 category of protection needs.

Implementation guidance

The data security concept should cover the risks arising from specific circumstances of the cloud service, its data processing operations, and its premises and include various security measures and specify resources, responsibilities, and prioritisations for handling information security risks. 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 may 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 into account all conceivable threats and security gaps;

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 whether a countermeasure is required.

The data security concept should be continuously updated and improved, taking into account emerging security challenges. Risk assessments, the possible level of damage, and the identified acceptable risks should be regularly reviewed, taking into account changes in the organisation, technology, business objectives and processes, identified threats, the impact of implemented controls, and external events.

Demonstrating compliance

The cloud provider can demonstrate compliance with the data security concept and its appropriateness by submitting it.

No. 2.2 – security area and entry control (Art. 32 para. 1 lit. b and para. 2 in connection with Art. 5 para. 1 lit. f GDPR)

Criterion

Protection category 1

(1) The cloud provider ensures, with risk-appropriate TOM, that premises and equipment are protected against damage caused by acts of god[3], and that unauthorised persons have no entry to premises and data processing equipment in order to prevent unauthorised inspection of personal data and the possibility of influencing the data processing equipment.

(2) The measures are generally appropriate for excluding entry by unauthorised persons due to technical or organisational errors, including operating errors, of the cloud provider or due to acts of negligence of third parties. A minimum level of protection must be provided to make intentional interferences more difficult to achieve.

Protection category 2

(3) The criteria of protection category 1 are fulfilled.

(4) The measures are appropriate for generally excluding damage caused by negligent actions of authorised persons. It is further ensured that unauthorised entry through negligent and intentional actions is excluded with sufficient certainty. That includes protection against entry attempts through deception and force. There is adequate protection against known attack scenarios.

(5) Every unauthorised entry and entry attempt can be detected subsequently.

Protection category 3

(6) The criteria of protection category 1 and protection category 2 are fulfilled.

(7) Every authorised entry is logged.

Explanation

This criterion partially substantiates the obligation contained in Art. 32 para. 1 lit. b and Art. 5 para. 1 lit. f GDPR to ensure the protection goals of integrity, confidentiality, and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation. Insofar as the cloud provider is responsible for the security area and the entry control to premises and data processing equipment, it will require an authorisation concept for entry to data processing equipment. Entry control ensures entry protection not only during normal operation, but also in connection with acts of god.

Implementation guidance

The implementation guidance under ISO/IEC 27001 no. A11 and ISO/IEC 27018 no. 11 is applicable.

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

To ensure that unauthorised persons cannot enter the premises and data processing equipment, entry to the data centre should be permanently monitored with video surveillance systems, motion sensors, alarm systems, and trained security personnel.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting the TOMs for entry control in the data security concept.

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

Criterion

Protection category 1

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

(2) The cloud provider shall periodically review and, if necessary, update the timeliness and adequacy of authorisations required for admission to data processing systems.

(3) The cloud provider shall verify the admission of authorised persons via the Internet through strong authentication that uses at least two elements of the categories knowledge, possession, or inherence. The elements are independent of each other, so overcoming one element does not affect the reliability of the other. They are designed in such a way that the confidentiality of the authentication data is guaranteed. Admission via the Internet occurs via an encrypted communication channel.

(4) As a rule, the measures for admission control are appropriate for excluding admission to data processing systems 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 is provided to make intentional interferences more difficult to achieve.

Protection category 2

(5) The criteria of protection category 1 are fulfilled.

(6) Protection exists against expected intentional unauthorised admission which excludes expected admission attempts with sufficient certainty. This includes adequate protection against known attack scenarios in particular as well as measures through which unauthorised admissions can normally be detected (subsequently).

Protection category 3

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

(8) The cloud provider excludes unauthorised admission to data processing systems with sufficient certainty. This includes regular measures to actively recognise attacks. Every unauthorised admission and attempt can be detected subsequently.

Explanation

The criterion of admission control partially substantiates the obligation contained in Art. 32 para 1. lit. b and para. 2 GDPR to ensure the protection goals of integrity, confidentiality, and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation. Insofar as the cloud provider is responsible for data processing system access, it will require an authorisation concept for data processing system access.

Implementation guidance

The implementation guidance under ISO/IEC 27001 no. A12.1.4, A12.4.2 and ISO/IEC 27018 no. 9 is applicable.

The tasks and roles for safeguarding information security for the cloud provider's data processing operations should be clearly defined and documented. All of the cloud provider's equipment should be properly maintained to ensure its continued availability and integrity.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting the TOMs for admission control in the data security concept.

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

Criterion

Protection category 1

(1) The cloud provider shall ensure through TOMs that authorised persons can only access personal data as part 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 controls any access to personal data.

(3) As a rule, the measures are appropriate for excluding access to personal 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 is provided to make intentional interferences more difficult to achieve.

(4) For access to personal data via the Internet by authorised persons, strong authentication is required that uses at least two elements of the categories knowledge, possession, or inherence, which are independent of each other in such a way that overcoming one element does not compromise the reliability of the other and which are designed in such a way as to ensure the confidentiality of the authentication data.

(5) The cloud provider shall protect and log administrative access and activities on critical systems through a strong authentication mechanism. Remote administration of the cloud service through the cloud provider's employees is done via an encrypted communication channel.

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

Protection category 2

(7) The criteria of protection category 1 are fulfilled.

(8) Expected intentional unauthorised access is excluded with sufficient certainty. This includes adequate protection against known attack scenarios in particular as well as measures through which unauthorised access can normally be detected subsequently.

(9) The cloud provider ensures that the cloud user determines different purpose-related user roles for its employees in order to logically exclude inappropriate access to personal data.

(10) If the cloud provider's employees are to have privileged access to personal data as instructed, it must be clearly regulated and documented. Privileged access may only take place in roles that are independent of administration and data centre operation. Access must be secured with two-factor authentication, and the number of employees with privileged access must be kept as low as possible.

Protection category 3

(11) The criteria of protection category 1 and protection category 2 are fulfilled.

(12) Unauthorised data access is excluded with sufficient certainty. This includes regular measures to actively recognise attacks. Any unauthorised access and related attempts can be detected subsequently.

Explanation

The criterion of access control partially substantiates the obligation contained in Art. 32 para 1. lit. b and para. 2 GDPR to ensure the protection goals of integrity, confidentiality, and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation. This requires an authorisation concept for access to personal data.

Implementation guidance

The implementation guidance under ISO/IEC 27002 no. 13.2 and ISO/IEC 27018 no. 9.2, 9.2.1, 9.4.2 is applicable.

Authorisation concepts must exist for both the users of the service and the employees of the cloud provider.

A appropriate management process for access control should be established that regularly reviews the appropriateness of the need for authorisations, regulates the allocation, updating, control, and withdrawal of authorisations, monitors and updates access policies, reviews password policies, 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, antivirus, regular integrity checks of important system files, and host-based intrusion detection systems. The cloud service should be continuously monitored for attacks and security incidents in order to detect suspicious activities (e.g. extraction of large amounts of data from multiple clients), attacks, and security incidents in a timely manner and to initiate appropriate and timely responses.

So as to make it more difficult for employees to intentionally interfere with data processing operations, the circle of authorised persons must 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 complete 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. In order to be able to subsequently track accesses by authorised employees, every access must be logged.

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

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting the TOMs for access control in the data security concept.

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

Criterion

Protection category 1

(1) The cloud provider uses state-of-the-art transport encryption or equally appropriate measures for data transfer processes or requires this through an appropriate configuration of interfaces. The used transport encryption ensures that personal data cannot be read, copied, modified, or deleted during electronic transmission without authorisation.

(2) As a rule, the measures are appropriate for excluding attacks by unauthorised persons due to technical or organisational errors, including operating errors, of the cloud provider or its employees or due to acts of negligence of the cloud user or third parties. Moreover, the measures are suitable for excluding the negligent disclosure of data to unauthorised persons by the cloud provider and its employees. A minimum level of protection is provided to make intentional interferences more difficult to achieve. Where the transmission is encrypted, the encryption keys must be securely stored.

(3) The cloud provider automatically logs the metadata of all data transfer operations, including those of recipients and those 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 protects the transport of data media with TOMs so that personal data cannot be read, copied, modified, or deleted without authorisation while transporting the data media. The cloud provider keeps records of the transports.

Protection category 2

(6) The criteria of protection category 1 are fulfilled.

(7) The cloud provider protects the data from intentional unauthorised reading, copying, alteration, or deleting and excludes expected attempts with sufficient certainty. The protection measures include adequate protection against known attack scenarios in particular as well as measures through which unauthorised reading, copying, alteration, or deleting can normally be detected (subsequently).

Protection category 3

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

(9) The cloud provider excludes 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. Where encrypted transmission is used, the cloud provider uses TOMs to ensure that neither the cloud provider nor its employees have access to the encryption keys.

Explanation

The criterion of transmission and transport control specifies the obligation contained in Art. 32 para.1 lit. b and para. 2 GDPR to ensure the protection goals of integrity, confidentiality, and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation, and to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised admission or disclosure during electronic transmission, transport, or storage on data media.

Implementation guidance

The implementation guidance under ISO/IEC 27018 no. 10.1.1, A.10.6, A.10.9, ISO/IEC 27002 no. 12.4, ISO/IEC 27040:2017-03 no. 6.7.1 and ISO/IEC 27040:2017-03 no. 7.7.1 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting the TOMs for transmission control in the data security concept.

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

Criterion

Protection category 1

(1) The cloud provider logs 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, in order to ensure that data processing can be subsequently verified and traced. The cloud provider observes the principles of necessity, purpose limitation, and data minimisation for logging and stores the log data securely.

(2) The cloud provider designs the logs in such a way that entries, alterations, and erasures can be traced as a rule, even in the event of technical or organisational errors, including operating errors, of the cloud provider or its employees or negligent actions of the cloud user or third parties. The cloud provider provides 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 are fulfilled.

(4) The cloud provider provides protection against expected intentional manipulation of logging instances and against intentional access to or manipulation of logs by unauthorised persons, which excludes expected manipulation attempts with sufficient certainty. These protection measures include adequate protection against known attack scenarios in particular as well as measures through which manipulation can normally be detected subsequently.

Protection category 3

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

(6) The cloud provider excludes manipulation of the logging authority and logs with sufficient certainty. It regularly takes measures to actively detect manipulations and subsequently detects every manipulation and, if possible, every related attempt.

Explanation

The criterion of traceability partially specifies the obligation contained in Art. 32 para. 1 lit. b and para. 2 GDPR to ensure the protection goals of integrity, confidentiality and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation, and to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised admission or disclosure. To this end, it must be possible to subsequently check and establish whether, and when and by whom and with what effect on content, personal data has been entered, modified, or removed in data processing systems in order to change access rights for the future, if necessary. The secure retention of log data also includes ensuring that the log data can be evaluated.

Because personal data is 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 minimisation and purpose limitation protection goals under Art. 5 para. 1 lit. c and b GDPR.

Implementation guidance

The implementation guidance under ISO/IEC 27018 no. 12.4.1, 12.4.2 and ISO/IEC 27002 no. 12.4 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept how it ensures data protection objectives by defining the subject-matter and scope of logging, retention, and use of the log data, integrity protection, and deletion of logs.

No. 2.7 – Pseudonymisation (Art. 32 para. 1 lit. a GDPR)

Criterion

Protection category 1

(1) The cloud provider shall enable the cloud user to process data that the cloud user transfers pseudonymised.

Protection category 2 and 3

(2) The cloud provider shall ensure that data can be processed pseudonymised. Pursuant to the legally binding agreement (No. 1.7), the cloud user pseudonymises the personal data itself, or the cloud provider conducts 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 are kept separate. The data record that assigns identifiers to a person must be protected in such a way that expected manipulation attempts are excluded with sufficient certainty.

(4) Where the type of processing with the cloud user requires the de-pseudonymisation of the data, the cloud provider ensures that the de-pseudonymisation only takes place on the cloud user's documented instructions.

(5) The cloud provider shall guarantee that it continuously monitors technical developments in the field of pseudonymisation mechanism and that its procedures comply with best practice standards.

Explanatory notes

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 does have to process pseudonymous data while maintaining pseudonymity.

In addition to encryption, pseudonymisation of personal data is explicitly mentioned in Art. 32 para.1 lit. a GDPR as being a security measure to be implemented. It contributes to promoting the protection goal of unlinkability (SDM 6.2.4). Since pseudonymisation prevents third parties from gaining knowledge of personal data, even when gaining unauthorised access to the cloud service, or at least makes it considerably more difficult to identify persons, pseudonymisation reduces the risks to the fundamental rights and freedoms of the data subjects.

Implementation guidance

The cloud user must examine whether there are sector-specific or generic technical standards for pseudonymisation that are mandatory or recommended. The cloud provider should publicly announce which of these technical standards it uses as its pseudonymisation mechanism. For example, DIN EN ISO 25237 can be referred to for pseudonymisation in medical informatics.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept how it carries out pseudonymisation, keeps identification data safe, and processes pseudonymised data.

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

Criterion

Protection category 1

(1) The cloud provider shall 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 ensures that the data are processed in an anonymised manner. In accordance with the legally binding agreement, the cloud user anonymises the personal data itself, or the cloud provider does so upon instruction.

(3) If the anonymisation is carried out by the cloud provider, the cloud provider ensures that it continuously follows the technical developments in the field of anonymisation processes, and that its processes are on the level of best practice standards. The anonymisation must exclude a re-identification of the data subject according to the state of the art.

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 does have to process anonymous data while maintaining anonymity.

Besides forgoing data collection, anonymisation is the most effective measure for data avoidance and data minimisation. It contributes to promoting the protection goal of data minimisation (SDM 7.1).

Implementation guidance

The cloud user should examine whether there are sector-specific or technical standards for anonymisation that are mandatory or recommended. The cloud provider should publicly announce which of these technical standards it uses as its anonymisation mechanism.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept how it carries out anonymisation and processes anonymised data.

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

Criterion

Protection category 1

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

Protection category 2

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

(3) The cloud provider continuously monitors technical developments in encryption. The measures the cloud provider takes comply with best practice standards.

(4) The cloud provider continuously checks the suitability of its encryption methods and updates them as needed.

(5) The cloud provider verifies the appropriate implementation of its encryption methods through suitable tests and documents them.

Protection category 3

(6) On the cloud user's instructions, the cloud provider must assist the cloud user with encrypting and decrypting data. Assistance is given by way of documentation and support for implementing encryption, without the cloud provider being able to know the encryption key.

(7) The cloud provider monitors technical developments in encryption and ensures that its support measures in the form of documentation and supporting measures for implementing encryption on the level of best practice standards.

Explanation

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 does have to store encrypted data while maintaining encryption.

In protection category 3, the cloud user encrypts the data itself. It is therefore also the user's responsibility to keep the encryption keys safe.

In addition to pseudonymisation, encryption of personal data is explicitly mentioned in Art. 32 para. 1 lit. a GDPR as being a security measure to be implemented. The purpose of encryption is to ensure the protections goals of confidentiality and integrity (SDM 6.2.2 and 6.2.2). The threshold above which encryption is required is low, so that, where possible, personal data should be encrypted when there is a low risk.

Implementation guidance

The state-of-the-art results from current technical standards for cryptographic procedures and their application. The implementation guidance under ISO/IEC 27018 no. 10 and ISO/IEC 27002 no. 10 is applicable.

Where the cloud provider encrypts its data, encryption keys should be generated in a secure environment using appropriate key generators. If possible, cryptographic keys should serve only one purpose and should generally never be stored as a clear key type but should always be encrypted in the system. A redundant and recoverable backup system must be used for storage in order to prevent the loss of a key. Key changes must be carried out on a regular basis. Admission to the encryption key administration system should require separate authentication. Cloud administrators may not have access to user keys.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept that the offered and applied encryption procedures correspond to current technical requirements. The cloud provider shall provide process documentation on how it monitors technical encryption developments and must further keep the suitability of the procedure under review and update it where necessary. In its data security concept, the provider must demonstrate that it has tested the encryption techniques of protection category 2 services through appropriate technical tests.

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

Criterion

Protection category 1

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

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

Protection category 2

(3) The criteria of protection category 1 are fulfilled.

(4) The cloud provider offers protection against expected intentional violations with sufficient certainty. In the context of data storage, this includes encryption with individual keys and the use of separate operating environments for different processing operations or the use of equivalent procedures. As a rule, the cloud provider can (subsequently) detect intentional violations of the separation rule, e.g. by logging accesses.

Protection category 3

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

(6) The cloud provider excludes a violation of data separation with sufficient certainty. In the context of data storage, this includes encryption with separate encryption keys and the use of separate operating environments for different processing operations or the use of equivalent procedures. The provider operates a procedure for detecting intentional violations of separate processing.

Explanation

The criterion promotes the protection goals of availability, integrity, confidentiality and unlinkability (SDM 6.2.1-6.2.4) and therefore also aims to ensure the principle of purpose limitation from Art. 5 para. 1 lit. b GDPR. Secure client separation protects the data from unauthorised access, alterations, and destruction and prevents an unwanted linking of the data.

Regarding the separation of the data processing in accordance with different purposes of processing, it must be observed that the cloud provider must only 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

The implementation guidance under ISO/IEC 27002 no. 12.1.4, 13.1.3 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept which TOMs it has taken to separate the data of different users from each other and to be able to separate the data of a user according to the purposes of the processing.

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

Criterion

(1) Through risk-appropriate TOMs, the cloud provider shall ensure that after a physical or technical incident, the cloud service and the data are recovered and made available as quickly as agreed in the legally binding data processing agreement. A distinction is made between the restorability classes 1, 2, and 3:

Restorability class 1

The cloud provider provides such reliable protection for its service against expected and probable events that these risks do not lead to a failure of the cloud service or a final loss of data in the normal course of events. Events are to be expected and obvious when they are not supposed to happen but, as experience has shown, cannot be ruled out despite using sufficient caution; examples are traffic accidents or the technical defect of hardware.

Restorability class 2

The cloud provider provides such reliable protection for its service against rare events that these risks do 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 when they are not supposed to happen and, as experience has shown, are unlikely when exercising sufficient caution but can nevertheless be observed 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 guarantees a high level of protection for its service, which provides such reliable protection against exceptional albeit not theoretically impossible events so that these risks do 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, as experience has shown, do not occur but can nevertheless be observed in extremely seldom isolated cases, such as black swan events or an uncontrollable lightning strike at the data centre.

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

Explanation

The criterion promotes the protection goal of availability (SDM 6.2.1). In accordance with Art. 32 para. 1 lit. c GDPR, the recovery must take place "in a timely manner". What constitutes "in a timely manner" depends on the severity of the incident and the significance of the systems and data. The cloud user must be able to select which recovery time frame is sufficient. For instance, the requirements for the recoverability 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 its protection need on the basis of the concept of protection categories, there could be a requirement on the part of the cloud user for personal data in protection category 1 to be very quickly recovered after a physical or technical incident, this criterion is not decided upon according to 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 restorability after a physical or technical incident is not about normal operations, as is the case with the other criteria in number 2, but about physical or technical incidents.

Natural events, infrastructure disruptions and malfunctions, operating errors and intentional interference are considered events.

Implementation guidance

To recover data and systems, a cloud provider should develop an effective data protection concept that includes backup systems, emergency management, recovery and mitigation plans, and a plan to periodically review and update the planned actions.

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 implementation guidance under ISO/IEC 27018 no. 12.3.1, A.10.3 is applicable for establishing a data protection concept.

The data protection strategies and measures of the data protection 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.

In addition to creating backup copies, the cloud provider should establish an emergency management system with corresponding emergency plans. This includes identifying and evaluating potential disruptions so that recovery and damage mitigation plans can be developed and used in an emergency. The developed emergency plans must be continuously updated and tested for effectiveness in order to ensure the fastest possible response in the event of an interruption.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept which restorability times its service offers, which events it has dealt with that can lead to a physical, organisational or technical incident, and which specific measures it has taken to recover the data after an incident.

No. 3 – Ensuring compliance with issued instructions (Art. 28 para. 3 sentence 2 lit. a; 29 GDPR)

Criterion

Protection category 1

(1) The cloud provider carries out the data processing by order only upon the documented instruction of the cloud user.

(2) The cloud provider ensures that the processing of the cloud user's data is only carried out on the cloud user's instructions. As a rule, the provider excludes deviations from the issued instructions due to technical or organisational errors, including operating errors, of the cloud provider or its employees or due to acts of negligence of the cloud user or third parties. A minimum level of protection must be provided to make a manipulation of issued instructions more difficult.

(3) Within the framework of standardised bulk transactions, the cloud provider guarantees the observance of a specific and comprehensible service description for the services it is technically able to carry out, so that the cloud user can assign the cloud provider via its selection for order processing. In addition, it enables the cloud user to issue instructions by means of software orders, which are carried out automatically and documented.

Protection category 2

(4) The criteria of protection category 1 are fulfilled.

(5) The cloud provider excludes a deviation from the instructions through expected intentional interferences with sufficient certainty and, as a rule, determines interventions (subsequently).

Protection category 3

(6) The criteria of protection category 1 and protection category 2 are fulfilled.

(7) The cloud provider excludes deviations from the cloud user's instructions with sufficient certainty and continuously and comprehensively logs access by administrators.

Implementation guidance

The cloud provider instructs all employees whose activities are related to the processing of personal data to process under the contractually documented authorities (Art. 29 GDPR) and also ensures compliance with the issued instructions in any data processing chain. The cloud provider must regularly verify whether the cloud user's instructions are being complied with.

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

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept how it receives, implements, and documents the cloud user's instructions. For bulk transactions, the cloud provider must demonstrate compliance with the requirements for its specific service description on its technologically executable services and demonstrate compliance with the requirements for the executability of issued instructions through software commands in the form of technical documentation or through the use of services.

No. 4 – Reporting duty of the cloud provider

No. 4.1 – Instructions contrary to legal data protection provisions (Art. 28 para. 3 sentence 3 in connection with Art. 29)

Criterion

> The cloud provider will immediately inform the cloud user if it is of the opinion 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 may not carry out an instruction without scrutiny when it doubts its lawfulness. Rather, 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

When including instructions in the legally binding data processing agreement and when any instructions are issued after its conclusion, the cloud provider should consult its data protection officer if the data protection violation of the instruction is imposed on a cloud service employee trained in data protection law. The cloud provider has no obligation to review an instruction without cause.

For bulk transactions where the cloud user instructs the cloud provider by selecting the cloud service based on a service description of the cloud provider, the cloud provider must take TOMs to inform the cloud user if it is using this service contrary to the service description (e.g. does not use the data security measures provided by the cloud provider such as encryption and pseudonymisation).

The implementation guidance under ISO/IEC 27018 no. 16.1.1 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting how it checks instructions, how it recognises doubts as to their permissibility under data protection law, and how it informs the cloud user of this before executing the instructions.

No. 4.2 – Changes to the place of data processing (indirectly Art. 28 para. 3 sentence 2 lit. a GDPR)

Criterion

The cloud provider must notify the cloud user immediately in the event in which, during the period of validity of the agreement, the place of data processing changes from the one specified in the agreement (No. 1.5) for reasons in the area of responsibility of the cloud provider or which are unforeseeable for both parties.

Implementation guidance

For bulk transactions, a communication process should be set up, preferably supported by an automated information system within the cloud service such as on the cloud provider's website, allowing the cloud user to know where the data is being processed in the event of a change of place.

Demonstrating compliance

The cloud provider may demonstrate compliance with the requirements by documenting measures and responsibilities it has implemented to notify the cloud user of changes to the place of data processing.

No. 5 – Ensuring confidentiality amongst personnel (Art. 28 para. 3 sentence 2 lit. b GDPR)

Criterion

(1) The cloud provider introduces an organisational process in order to ensure that the persons authorised to process personal data are bound to confidentiality before the start of the data processing operation in accordance with the order processing agreement (No. 1.6), unless they are already subject to a suitably comparable statutory obligation of confidentiality.

(2) The organisational process also includes the documentation of the confidentiality declarations and their adjustment, if access and processing authorisation change.

Explanation

The confidentiality obligation and secrecy instruction promote the protection goal of confidentiality (SDM 6.2.3)

Implementation guidance

The cloud provider should provide its employees a copy of the declaration of obligation while pointing out the possible consequences of a breach to an obligation of confidentiality. The provider should repeat the information at appropriate intervals, e.g. in connection with training courses or if the access and processing competence of the employee changes. Furthermore, the cloud provider should regularly raise the data subjects' awareness of data protection and data security issues in relation to their activities.

In the documentation of the process, the cloud provider should determine who is responsible for providing the information and carrying out obligations, when and how this is carried out, which persons must be obligated and informed at what time, and what evidence of the obligation and information is kept where and for how long.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting information and obligations along with all relevant processes and responsibilities.

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

No. 6.1 – Provision of information (Art. 28 para. 3 lit. e in connection with Art. 15)

Criterion

(1) The cloud provider ensures that the cloud user has the opportunity to provide data subjects with information about the data processing and give them a copy of the personal data, or arrange this via the cloud provider.

(2) The cloud provider documents instructions to implement the rights of the data subject.

(3) The cloud provider is exempt from the duty to grant information in cases in which the responsibility lies with the cloud user, and this party is in charge of applications and files.

Explanation

In accordance with Art. 15 GDPR, the cloud user is obliged to grant the data subject information about data processing and its situation, upon request. The cloud provider must assist the cloud user, with appropriate TOM, in the exercise of the rights of data subjects. This criterion promotes the protection goals of transparency and intervenability (SDM 6.2.5 and 6.2.6).

Implementation guidance

Where it is not possible for the cloud user to implement the rights of the data subject itself, an organisational point of contact should be provided for the cloud user, which can arrange for the immediate implementation of the rights of the data subject through appropriate availability and authority.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to enable the cloud user to provide information to a data subject or to have the cloud provider provide the information. Whether the information was actually provided can also be verified by means of process documentation.

No. 6.2 – Rectification and completion (Art. 28 para. 3 lit. e in connection with Art. 16 GDPR)

Criterion

(1) The cloud provider ensures, with appropriate measures, that the cloud user has the opportunity to carry out the rectification and completion of personal data itself, or have it carried out by the cloud provider.

(2) The cloud provider documents instructions to implement the rights of the data subject.

(3) The cloud provider is exempt from the rectification and completion obligations in cases in which the responsibility lies with the cloud user, and the cloud user is in charge of applications and files.

Explanation

In accordance with Art. 16 GDPR, the cloud user is obliged to rectify incorrect personal data and complete incomplete personal data, upon request. The cloud provider is obliged to assist the cloud user, with appropriate TOM, in the exercise of the rights of data subjects. The rectification in accordance with Art. 16 GDPR promotes the protection goal of intervenability (SDM 6.2.6).

Implementation guidance

Where it is not possible for the cloud user to implement the rights of the data subject itself, an organisational point of contact should be provided for the cloud user, which can arrange for the immediate implementation of the rights of the data subject through appropriate availability and authority.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to enable the cloud user to rectify and complete data or to have the cloud provider do so. Whether the data was actually rectified and completed can also be verified by means of process documentation.

No. 6.3 – Erasure (Art. 28 para. 3 lit. e in connection with Art. 17 para. 1 GDPR)

Criterion

(1) The cloud provider ensures that the cloud user has the opportunity to carry out the erasure of personal data itself, or have it carried out by the cloud provider.

(2) The cloud provider documents instructions to implement the rights of the data subject.

(3) The cloud provider is exempt from the erasure obligation in cases in which the responsibility lies with the cloud user, and the cloud user party is in charge of applications and files.

Explanation

In accordance with Art. 17 para. 1 GDPR, the cloud user is obliged to erase personal data. The cloud provider is obliged to assist the cloud user, with appropriate TOM, in the exercise of the rights of data subjects. This criterion promotes the protection goals of intervenability and unlinkability (SDM 6.2.4 and 6.2.6).

Implementation guidance

The implementation guidance under ISO/IEC 27040:2017-03 on data erasure no. 6.8.1 is applicable.

It is recommended to prepare an erasure concept, e.g. according to DIN 66398-2016. This may include the establishment 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. The measures under DIN 66398 for the preparation of an erasure concept and DIN 66993 for the destruction of data media can be consulted.

All of the cloud provider's data media should be disposed of safely and securely through the use of a formal management procedure when they are no longer needed.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to enable the cloud user to erase data or to have the cloud provider do so. Whether the erasure actually took place can also be verified by means of process documentation.

No. 6.4 – Restrictions of processing (Art. 28 para. 3 lit. e in connection with Art. 18 para. 1 GDPR)

Criterion

(1) The cloud provider ensures that the cloud user has the opportunity to restrict the processing of personal data itself, or have the restriction carried out by the cloud provider.

(2) The cloud provider documents instructions to implement the rights of the data subject.

(3) The cloud provider is exempt from the restriction of processing in cases in which the responsibility lies with the cloud user, and the cloud user is in charge of applications and files.

Explanation

In accordance with Art. 18 para. 1 GDPR, the cloud user is obliged to restrict the processing of personal data under certain conditions. The cloud provider is obliged to assist the cloud user, with appropriate TOM, in the exercise of the rights of data subjects. The criterion supports the protection goal of intervenability (SDM 6.2.6).

Implementation guidance

Where it is not possible for the cloud user to implement the rights of the data subject itself, an organisational point of contact should be provided for the cloud user, which can arrange for the immediate implementation of the rights of the data subject through appropriate availability and authority.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to enable the cloud user to restrict processing or to have the cloud provider do so.

No. 6.5 – Notification obligation in the event of rectification, erasure or restriction of processing (Art. 28 para. 3 lit e. in connection with Art. 19 GDPR)

Criterion

(1) The cloud provider ensures that the cloud user has the opportunity to notify recipients, to whom it has disclosed personal data, of any rectification, erasure or restriction of processing, or have the notification provided by the cloud provider, and inform the data subject of the recipients, upon request.

(2) The cloud provider documents instructions to implement the rights of the data subject.

(3) The cloud provider is exempt from the duty to inform in cases in which the responsibility lies with the cloud user, and the cloud user is in charge of applications and files.

Explanation

In accordance with Art. 19 GDPR, the cloud user is obliged to inform recipients, to whom it has disclosed personal data, about any rectification, erasure or restriction of processing, and inform the data subject about the recipients, upon request. If the cloud provider was involved in the disclosure, it is obliged to assist the cloud user, with appropriate TOM, in the exercise of the rights of data subjects. This criterion promotes the protection goals of transparency and intervenability (SDM 6.2.5 and 6.2.6).

Implementation guidance

Where it is not possible for the cloud user to implement the rights of the data subject itself, an organisational point of contact should be provided for the cloud user, which can arrange for the immediate implementation of the rights of the data subject through appropriate availability and authority.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to enable the cloud user 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 or to have the cloud provider do so.

No. 6.6 – Data transmission (Art. 28 para. 3 lit. e in connection with Art. 20 para. 1 and 2 GDPR)

Criterion

(1) The cloud provider ensures that the cloud user has the opportunity 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 have it transmitted by the cloud provider.

(2) The cloud provider documents instructions to implement the rights of the data subject.

(3) The cloud provider is exempt from the data transmission in cases in which the responsibility lies with the cloud user, and this party is in charge of applications and files.

Explanation

Pursuant to Art. 20 para. 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. The cloud provider should list the commonly used formats it can use in the legally binding agreement for clarity.

The cloud provider is obligated to assist the cloud user in fulfilling the rights of data subjects through the use of appropriate TOMs. The criterion promotes the protection goal of intervenability (SDM 6.2.6).

Implementation guidance

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

Where it is not possible for the cloud user to implement the rights of the data subject itself, an organisational point of contact should be provided for the cloud user, which can arrange for the immediate implementation of the rights of the data subject through appropriate availability and authority.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to enable the cloud user to transmit the data provided by a data subject to this person or another controller in a structured, commonly used and machine-readable format or to transmit these data by the cloud-provider.

No. 6.7 – Objection (Art. 28 para. 3 lit. e in connection with Art. 21 para. 1 and Art. 32 para. 1 lit. b GDPR)

Criterion

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

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

(3) The cloud provider documents instructions to implement the rights of the data subject.

(4) Exceptions are cases in which the responsibility lies with the cloud user, and the cloud user is in charge of applications and files.

Explanation

Under Art. 21 GDPR, the data subject has the right to object to processing of personal data concerning him or her. 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 through the use of appropriate TOMs. The criterion promotes the protection goal of intervenability (SDM 6.2.6).

Implementation guidance

The cloud provider should have a policy in place that lays down 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.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has implemented to make the necessary data available to the cloud user.

No. 7 – Assisting in data protection impact assessment (Art. 28 para. 3 lit. f in connection with Art. 35 and 36 GDPR)

Criterion

(1) The cloud provider assists the cloud user in the execution 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 risk-appropriate precautions.

(3) The cloud provider provides the cloud user with all information that falls within its area of responsibility and that the cloud user requires for its data protection impact assessment.

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

Explanation

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

Implementation guidance

The assistance obligations for the data protection impact assessment should be aligned with 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, if they are not already apparent from the service description of the cloud provider.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting how it can assist the cloud user through relevant information. The cloud provider should demonstrate that this information is available or can be generated by the cloud provider quickly.

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 37-39 GDPR. The ensurance of a data protection management system should aid the constant ensurance 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. 37–39 GDPR, Sec. 38 BDSG)

Criterion

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

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

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

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

(5) The cloud provider ensures the acknowledgement of the person and function of the DPO in the organisation structure and supports him in his tasks, in particular with appropriate resources.

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

(7) If an information security officer has been designated, the officer shall ensure compliance with TOMs required under data protection law. The cloud provider ensures that the DPO and the information security officer cooperate in an appropriate manner (mutual information and assistance).

Explanation

If cloud providers are obliged to designate a DPO, they must carefully select, equip and protect him, and allocate him the place he merits within the company organisation.

The designation of an information security officer is not required by the General Data Protection Regulation. However, the cloud provider may be obliged to designate one on the basis of other duties, or carry out the designation voluntarily.

If a DPO is designated, the DPO must comply with its 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 should provide as accurate a description as possible of the TOMs as a whole (e.g. in a data security concept), making this available to the DPO and, upon request, to the supervisory authority.

Where the DPO is employed by another company (external DPO of the cloud provider) or is the DPO of other companies simultaneously, the DPO's freedom from instruction 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 that could result in a conflict of interests. Conflicts of interest are to be assumed as part of the following activities: Activities within the scope of which the DPO would have to monitor himself/herself, e.g. position as a managing director, IT or HR manager, information security officer, economic interests of the DPO in the success of the company, too close to the designating body.

The DPO's obligation of confidentiality includes, but is not limited to, the identity of the complainant or data subject(s), all information relevant to data protection laws, and anything that might lead to the identification of a person who can provide information. The DPO is also obligated to maintain secrecy vis-à-vis the designating body. The criterion promotes the protection goal of confidentiality (SDM 6.2.3).

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by having designated a DPO and by presenting the DPO's direct accessibility to the public through information on its website. The cloud provider may submit relevant certificates and assessments to assess the DPO's professional and personal suitability. The DPO's regular internal audits demonstrate its activities, its independence, and its involvement and effectiveness in the cloud provider's organisational structure.

No. 8.2 – Notification of a personal data breach (Art. 33 para 2 and Art. 28 para. 3 lit. f GDPR)

Criterion

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

(2) The cloud provider determines who is responsible for deciding on and carrying out the notification to the cloud user. The competent authorities shall 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 have sufficient resources to ensure that notifications are processed without undue delay. The employees in the responsible departments are sufficiently trained to be able to assess violations and carry out an impact assessment.

Explanation

Pursuant to Art. 33 para. 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 to the supervisory authority under Art. 33 para. 1 GDPR and its obligation to communicate the violation to the data subjects under Art. 34 para. 1 GDPR. This obligation also applies to sub-processor violations throughout the sub-processing chain. The criterion promotes the protection goal of integrity and transparency (SDM 6.2.2 and 6.2.5).

Implementation guidance

The notification of personal data breaches can be done using appropriate information systems within the service, such as messaging systems or news messages.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept how it ensures the notification of personal data breaches.

No. 8.3 – Maintaining records of processing activities (Art. 30 para. 2 GDPR)

Criterion

(1) Cloud providers that employ 250 persons or more shall maintain records of processing activities. The cloud provider shall maintain a record of processing activities, regardless of the number of employees, if the processing involves risks to the rights and freedoms of the data subjects.

(2) The cloud provider shall maintain a record of all categories of processing operations carried out on the behalf of a controller. The record shall further contain the content listed in Art. 30 para. 2 GDPR.

(3) An individual record of processing activities must be kept for every single cloud user.

(4) The record of processing activities must be kept in writing or in an electronic form. It must be made available to the supervisory authority upon request.

Explanation

The criterion promotes the protection goal of transparency (SDM 6.2.5).

If the processing operation is likely to result in a risk to the rights and freedoms of data subjects, or the processing includes special categories of personal data as referred to in Art. 9 or 10 GDPR, then the processing operation is risky within the meaning of Art. 30 para. 5 GDPR. Cloud providers employing fewer than 250 persons will also generally have to keep records of processing activities, as risks arise from the amount of data processed and data processing does not take place only occasionally, making the exception under Art. 30 para. 5 GDPR generally not applicable.

Implementation guidance

The records of processing activities to be maintained for each cloud user should also document the TOMs used for each cloud user to ensure data security during data processing. In the case of standardised bulk transactions, the records of processing activities should be created automatically.

The procedure record 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 directed exclusively internally and towards the relationship with the supervisory authority. The cloud user should, however, get insight into the report relating to its contract, e.g. for audits and inspections under Art. 28 para. 3 sentence 2 lit. h GDPR.

The implementation guidance under ISO/IEC 27018 no. A5.2 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting (a representative sample of) the records of processing activities.

No. 8.4 – Return of data media and erasure of data (Art. 28 para. 3 lit. h GDPR)

Criterion

The cloud provider ensures, with appropriate measures, that the return of provided data media, the return of data, and the 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.

Implementation guidance

Reference is made to ISO/IEC 27018 no. A 9.3.

The implementation guidance under ISO/IEC 27040:2017-03 on data erasure no. 6.8.1 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which procedure it intends to use, according to which it will hand out data media, return data, and erase data at the end of processing. Furthermore, the cloud provider may provide acknowledgement of returns or automated communication of actual erasures of personal data no longer required for the data processing.

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

Criterion

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

(2) The cloud provider ensures, with appropriate TOM, 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 during the validity 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. 18.2.

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 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 for the (further) development and modification (in particular patches and system updates) of its service in order 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 management and release management should be clearly defined and aligned between cloud providers and cloud users.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which internal control system it has set up.

No. 8.6 – Selecting and using appropriate persons (Art. 28 para. 3 sentence 2 lit. e and f GDPR)

Criterion

(1) The cloud provider entrusts only those employees to carry out processing operations who are qualified to carry out their respective tasks, are reliable, and are aware of the importance of and are trained in both data protection and data security.

(2) The cloud provider ensures that there are no conflicts of interest amongst the employees regarding the performance of their respective tasks.

Explanation

The use of appropriate employees is a prerequisite 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

In order to maintain the specialised expertise of the employees, the cloud provider should conduct regular employee training workshops (approx. once a year) on data protection and information security issues, including the specific technology of the cloud service.

Demonstrating compliance

The cloud provider can demonstrate compliance with the required know-how of its employees by means of relevant qualifications. The cloud provider can demonstrate that employees have been trained and made aware of the importance of data protection by documenting the training workshops that have been conducted.

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 para. 1 in connection with Art. 5 para. 1 lit. f GDPR)

Criterion

(1) The cloud provider shall implement 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) within the scope of its offered service in a feasible and target-oriented manner.

(2) The cloud provider has 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 ensures that at all times, the traceability and transparency of the data processing, even in extended service chains by any sub-processor relationships, is guaranteed by its system design in the offered applications and by the service concept.

Explanation

As the controller, the cloud user must fulfil the design obligations under Art. 25 para. 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 such a way that they best support the data protection principles of Art. 5 GDPR.

Demonstrating compliance

The cloud provider provides documentation that shows which measures it has taken to implement the data protection principles when designing the cloud service. The documentation also describes the considerations that have been taken to determine the measures.

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

Criterion

(1) The cloud provider ensures that, by default, personal data is only accessible to the extent necessary to fulfil the processing purpose of the cloud user.

(2) The cloud provider ensures, by default, that personal data is not made accessible without the individual's intervention to an indefinite number of natural persons and that no risks arise for the data subject as a result of making personal data available in a too comprehensive way.

Explanation

The controller must comply with the duties under Art. 25 para. 2 GDPR. As soon as it has had data processing carried out on its behalf, the cloud user must select a cloud provider that fulfils this duty. The default settings of the cloud service must therefore be selected in such a way that they fulfil the duty under Art. 25 para. 2 sentence 1 GDPR.

Implementation guidance

The default settings should be designed in such a way that only personal data, the processing of which is necessary for the specific purpose of processing in question, is collected, stored, and made accessible. Insofar as the cloud provider has carried out a data protection impact assessment, requirements for the default settings may arise from the obligation to minimise the identified risks.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which internal control system it has set up.

Chapter V: Sub-processing

Explanatory notes

For processing on behalf of the controller, the principle of the provision of the most personal service possible applies. Under certain conditions, the cloud provider may use other sub-processors. If a sub-processor uses other sub-processors, a multi-level sub-processing relationship will occur.

As the main processor, the cloud provider must, however, ensure that the sub-processor also fulfils all obligations that the cloud provider as the main processor must fulfil, 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 – Other processors of the cloud provider (sub-processing) (Art. 28 para. 2 GDPR)

Criterion

(1) The cloud provider ensures that a cloud service is only provided with the inclusion of sub-processors, if and to the extent that the cloud user has agreed to this sub-processing beforehand in writing or text form. Only sub-processes in which the other processor has the opportunity to gain knowledge of processed personal data require approval.

(2) The cloud provider ensures that the sub-processor also guarantees all TOM within the framework of its processing on behalf of the controller and complies with all obligations that the cloud provider must also fulfil as the main processor, unless it has hereby been legally exempted. The sub-processor must be able to demonstrate the same guarantees as the main processor.

Explanation

The quality assurance and compliance with data protection in the service chain must be guaranteed by the cloud provider. In particular, the sub-processor may not cause the safeguarding of data subjects' rights to be made more difficult.

Implementation guidance

For standardised bulk transactions, cloud users can be informed automatically of changes in sub-processing, e.g. via an automatically generated email. In the general terms and conditions of cloud providers for bulk transactions, for example, a general agreement can also be obtained in advance for any changes in sub-processing, which are reserved. As a result of the automated information mentioned above, every cloud user is entitled to terminate the contract at any time because an objection (within the meaning of Art. 28 para. 2 sentence 2 second half of the sentence GDPR) by an individual cloud user for the bulk transaction does not prevent the cloud provider from engaging another processor.

The implementation guidance under ISO/IEC 27002 no. 15 is applicable.

Demonstrating compliance

The cloud provider can demonstrate legal compliance with further data processing by submitting the consent of the cloud users and the contracts for further processing (sub-cloud contracts) together with the information required for the conformity check (duration, type and purpose, place of further processing, information on the additional processor and its service description).

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

Criterion

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

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

Demonstrating compliance

The cloud provider can demonstrate legal compliance with further data processing by submitting the legally binding data processing agreement and the legally binding data sub-processing agreement together with the information required for the conformity check (duration, type and purpose, place of further processing, information on the additional processor and its service description).

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

Criterion

(1) The cloud provider informs the cloud user about the identity of all sub-processors it involves at all levels (including the summons addresses).

(2) The cloud provider always informs the cloud user about any intended changes in relation to the involvement or replacement of other sub-processors and guarantees that the cloud user can make use of its right to object at all levels of the processing.

Explanation

During processing, it must be possible at all times for the cloud user to find out which sub-processors are located in which processing step, and what applications and services in relation to personal data are carried out by which sub-processors and at what processing levels.

Implementation guidance

As the main processor, the cloud provider should draw up a detailed documentation of the involved sub-processors for each extension of the data processing service chain, stating their identity, including their summons address and the carried-out activities to make clear which (sub-)processor is involved in each of the data protection-critical service parts and which processing operations are carried out by whom. This presupposes that the sub-processor informs the cloud provider about its integrated sub-processors and provide the necessary 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.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting how it can inform the cloud user of intended modifications on the part of the sub-processor. The cloud provider can also draw up a detailed documentation of the involved sub-processors, stating their identity, including their summons address and the activities carried out to make clear which (sub-)processor is involved in each of the data protection-critical service parts and which processing operations are carried out by whom.

No. 10.4 – Selection and controlling of the sub-processors (Art. 28 para. 4 sentence 1 GDPR)

Criterion

(1) The cloud provider ensures 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 is convinced that its sub-processors fulfil 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 must itself make sure that the sub-processors comply with the legal data protection requirements. Thus, the implementation guidance under ISO/IEC 27017 no. 15.1.2, 15.1.3 and ISO/IEC 27002 no. 15 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by providing certificates of the sub-supplier or other documents that guarantee compliance with the General Data Protection Regulation. A transparent service description of the sub-processor can be helpful.

No. 10.5 – Ensuring the assistance function (Art. 28 para. 4 sentence1 in connection with Art. 28 para. 3 sentence 2 GDPR)

Criterion

(1) The cloud provider ensures that even when (several) sub-processors are engaged, its support function is fulfilled to the extent agreed in addition to its obligations as the main processor.

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

Implementation guidance

The cloud provider should keep internal documentation and log the processing because of the increased risk of further processing. This also serves the self-regulation of the cloud provider in fulfilling its obligations in the next stages of the processing.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in which obligations it involves processors. Protocols on the fulfilment of obligations resulting from the involvement of additional processors are helpful.

Chapter VI: Processing outside the EU and EEA

No. 11 – data transfers

No. 11.1 – Appropriate safeguards for data transfers (Art. 46 para. 2 lit. f in connection with Art. 42 para. 1 and 2 GDPR)

Criterion

(1) The cloud provider only transfers personal data to third countries or international organisations if there is a decision by the European Commission in accordance with Art. 45 para. 3 GDPR for the recipient state or international organisation, stating that an adequate level of protection applies therein.

(2) Alternatively, the transmission can take place if the recipient demonstrates appropriate safeguards within the meaning of Art. 46 para. 2 GDPR, and the data subject has executable rights and effective legal remedies in the third country or against the international organisation. Appropriate safeguards are also provided in a certificate in accordance with Art. 42 para. 2 GDPR if legally binding and enforceable obligations of the cloud provider also exist in the third country regarding the applicability of appropriate safeguards, including those in relation to the rights of the data subjects.

Explanation

The processing (both when contracted out or of one's own responsibility) of data subjects' personal data in the EU or the EEA is only permitted outside the EU and the EEA under the conditions set out in Art. 44 et seq. GDPR. The same applies to the transfer of personal data to a third country or to an international organisation for which there is no recognised adequate level of protection.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting appropriate safeguards pursuant to Art. 46 para. 2 GDPR. Certification pursuant to Art. 42 para. 2 GDPR that corresponds to this criteria catalogue or a similar one can also be used to demonstrate compliance.

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

Criterion

(1) Cloud providers that do not have an establishment in the EU or the EEA, but for which the General Data Protection Regulation still applies under Art. 3 para. 2 GDPR, shall designate a representative in the EU or the EEA in writing. The representative shall 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 whose behaviour is monitored, are.

(2) The representative shall be mandated by the cloud provider to be addressed on all issues related to processing for the purposes of ensuring compliance with the General Data Protection Regulation and shall give the representative the necessary authority to act on behalf of and in place of the cloud provider to fulfil the obligations of the General Data Protection Regulation.

Explanation

The cloud provider can decide whether the representative should act in addition to the provider or as the sole contact person; this is to be communicated accordingly in relation to third parties. Where 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, but may also appoint a representative in a Member State with responsibility for several Member States as long as there are data subjects in that Member State.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by providing the written designation of the representative.

D. Criteria and implementation guidance for processing as as a controller

Chapter VII: The cloud provider as the controller

No. 12 – Ensuring compliance with data protection principles (Art. 5 para. 1 and 2 in connection with Art. 24 GDPR)

Criterion

(1) The cloud provider shall provide the cloud user with all information it needs to verify the lawfulness of the processing when processing personal data to provide the cloud service or to fulfil legal obligations (principle of transparency).

(2) The cloud provider shall clearly and precisely define the purposes of the respective data processing for providing the cloud service and for fulfilling legal obligations (principles of purpose specification and purpose limitation).

(3) The cloud provider shall only process the cloud user's personal data where this is required to achieve the specified purposes of the processing (principle of data minimisation).

(4) The cloud provider has TOMs at its disposal to verify, rectify, and erase inaccurate or incomplete personal data, which it processes for performing the cloud service and to fulfil legal obligations (principle of accuracy).

(5) The cloud provider shall only permit identification of data subjects for no longer than is necessary for achieving the specified purposes for carrying out the cloud service or for fulfilling legal obligations, and shall delete unnecessary data as soon as possible (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 produces a controlling effect, it is not sufficient to merely determine the performance of the contract under Art. 6 para.1 subpara.1 lit. b GDPR or the fulfilment of legal obligations under Art. 6 para.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. Only after this purpose specification can the other data protection principles produce effects.

Implementation guidance

The principle of transparency is fulfilled when the cloud provider complies with information and disclosure obligations concerning the processing of data (No. 15.1 and No. 15.2). In addition, transparency can be achieved through data protection by system design and by default (No. 20.1 and No. 20.2).

To comply with storage limitation, the cloud provider should establish storage periods for all data or categories of data, limited to the minimum necessary. In addition, time limits 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.

Demonstrating compliance

The cloud provider provides documentation showing the TOMs it has taken to ensure compliance with data protection principles.

No. 13 – Legal basis for data processing (Art. 6 para. 1 subpara. 1 lit. b and c in connection with Art. 6 para. 2 GDPR)

Criterion

The cloud provider processes personal data for the performance of a contract to which the cloud user is a party or in order to take steps at the request of the cloud user prior to entering into a contract or to comply with a legal obligation to which the controller is subject.

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 to provide the cloud service. The legal basis for data processing is therefore Art. 6 para. 1 subpara.1 lit. b GDPR. The statute permits data processing insofar as it is necessary for fulfilling a contract or for measures prior to entering into a contract. Handling data for the conclusion of a contract, for contract changes, and contract terminations constitutes the fulfilment of the contract. Data 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 para. 1 subpara.1 lit. b GDPR.

Where the cloud provider and cloud user conclude a contract on providing a cloud service, the cloud provider shall be obligated to process the cloud user's personal data due to commercial and tax law retention obligations. Art. 6 para. 1 subpara.1 lit. c GDPR allows processing necessary 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 para. 2 GDPR contains an opening clause for applying such regulations.

The cloud provider shall provide the cloud user with information concerning the legal basis for data processing as part of the information to be provided pursuant to Art. 13 para. 1 lit. c GDPR (No. 15.1).

Demonstrating compliance

As part of the certification, the cloud provider can provide all or a representative sample of legally binding agreements, which the cloud provider has concluded with the cloud user concerning the provision of the cloud service.

As part of the certification, the cloud provider provides an overview of the legal obligations it is subject to for data processing.

No. 14 – Ensuring data security through appropriate state-of-the-art TOMs

Explanation

Also with regard to data processing for the performance of the contract with the cloud user on the provision of the cloud service and for fulfilling legal obligations must the cloud provider ensure, through TOMs, that data is protected in accordance with its need for protection – above all against security-relevant destruction, loss and unauthorised disclosure.

Because the cloud provider will not regularly process personal data of protection category 3 by executing the contract with the cloud user and in order to fulfil legal obligations, criteria shall only be given for protection categories 1 and 2.

No. 14.1 – Data security concept (Art. 24, 25, 32 in connection with Art. 5 para. 1 lit. f GDPR)

Criterion

(1) The cloud provider shall conduct a risk analysis with regard to data security and has a data security concept that corresponds to its protection category and is appropriate for the specific risks of its data processing operations for providing the cloud user with the cloud service and for fulfilling legal obligations.

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

(3) The data security concept shall be documented in writing.

(4) The data security concept shall be reviewed at regular intervals to ensure that it is up to date and appropriate and shall be updated as necessary.

(5) Insofar as the cloud provider uses processors for performing the contract with the cloud user, the data security concept shall describe which data processing operations have been outsourced and are therefore subject to the processor's TOMs.

(6) 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

Also with regard to data processing for the performance of the cloud service and for the fulfilment of legal obligations must risks be excluded or at least minimised against accidental and unlawful destruction, loss, alteration, unauthorised disclosure and unauthorised access to personal data. In determining the specific measures, the cloud provider shall take into account not only the processing modalities and the probability and severity of the damage, but also the state of the art as well as the costs of 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 performing the contract with the cloud user and for fulfilling legal obligations, documenting the risk assessment approach and methodology. Any risk should be addressed by one or more protective measures.

When analysing risks, the following characteristics may 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 into account all conceivable threats and security gaps;

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 whether a countermeasure is required.

The data security concept should be continuously updated and improved, taking into account emerging security challenges. Risk assessments, the possible level of damage, and the identified acceptable risks should be regularly reviewed, taking into account changes in the organisation, technology, business objectives and processes, identified threats, the impact of implemented controls, and external events.

Demonstrating compliance

The cloud provider can demonstrate compliance with the data security concept and its appropriateness by submitting it.

No. 14.2 – Security area and entry control (Art. 32 para.1 lit. b and para. 2 in connection with Art. 5 para.1 lit. f GDPR)

Criterion

Protection category 1

(1) The cloud provider protects premises and equipment against damage caused by acts of god[4] and prevents unauthorised persons from gaining entry to premises and data processing equipment in order to prevent unauthorised inspection of personal data and the possibility of influencing the data processing equipment. As a rule, the TOMs must be appropriate for excluding entry by unauthorised persons due to technical or organisational errors, including operating errors, of the cloud provider or due to acts of negligence of third parties. A minimum level of protection must be provided to make intentional interferences more difficult to achieve.

Protection category 2

(2) The criteria of protection category 1 are fulfilled.

(3) As a rule, the TOMs are appropriate for excluding damage caused by the negligent actions of authorised persons. They exclude unauthorised entry through negligent and intentional actions with sufficient certainty. That also applies to entry attempts through deception and force. The TOMs ensure adequate protection against known attack scenarios.

(4) Every unauthorised entry and entry attempt is detected subsequently.

Explanation

This criterion partially substantiates the obligation contained in Art. 32 para.1 lit. b and Art. 5 para. 1 lit. f GDPR to ensure the protection goals of integrity, confidentiality, and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation. This requires an authorisation concept for entry to the data processing equipment. Entry control ensures entry protection not only during normal operation, but also in connection with acts of god.

Implementation guidance

The implementation guidance under ISO/IEC 27001 no. A11 and ISO/IEC 27018 no. 11 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting the TOMs for entry control in the data security concept.

No. 14.3 – Admission control (Art. 32 para. 1 lit. b and para 2 in connection with Art. 5 para. 1 lit. f GDPR)

Criterion

Protection category 1

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

(2) The cloud provider shall periodically review and, if necessary, update the timeliness and adequacy of authorisations required for admission to data processing systems.

(3) The cloud provider protects the admission of authorised persons via the Internet through strong authentication that uses at least two elements of the categories knowledge, possession, or inherence. The elements must be independent of each other so that overcoming one element

[4] Acts of god are unusual processes in nature that cannot be influenced by humans and are limited in time. Examples are lightning strikes, floods, drought.

does not affect the reliability of the other. They must be designed in such a way that the confidentiality of the authentication data is guaranteed. Admission via the Internet must occur via an encrypted communication channel.

(4) As a rule, the measures for admission control are appropriate for excluding admission to data processing systems 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.

Protection category 2

(5) The criteria of protection category 1 are fulfilled.

(6) Protection must be planned against expected intentional unauthorised admission which excludes expected admission attempts with sufficient certainty. The TOMs ensure adequate protection against known attack scenarios and subsequently detect unauthorised access in normal cases.

Explanation

The criterion of admission control partially substantiates the obligation contained in Art. 32 para. 1 lit. b and para. 2 GDPR to ensure the protection goals of integrity, confidentiality, and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation. This requires an authorisation concept for admission to the data processing systems.

Implementation guidance

The implementation guidance under ISO/IEC 27001 no. A12.1.4, A12.4.2 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting the TOMs for admission control in the data security concept.

No. 14.4 – Access control (Art. 32 para. 1 lit. b and para. 2 in connection with Art. 5 para. 1 lit. f GDPR)

Criterion

Protection category 1

(1) The cloud provider ensures through TOMs that authorised persons can only access personal data when they are authorised and excludes unauthorised influences on data processing operations. This also applies to backups insofar as they contain personal data.

(2) Any access to personal data must be controlled.

(3) As a rule, the TOMs are appropriate for excluding access to data systems 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 is provided to make intentional interferences more difficult to achieve.

(4) The cloud provider protects access by authorised persons via the Internet through strong authentication that uses at least two elements of the categories knowledge, possession, or inherence, which are independent of each other in such a way that overcoming one element does not compromise the reliability of the other and which are designed in such a way as to ensure the confidentiality of the authentication data.

Protection category 2

(5) The criteria of protection category 1 are fulfilled.

(6) Protection must be planned against expected intentional unauthorised access which excludes expected access attempts with sufficient certainty. The TOMs ensure adequate protection against known attack scenarios and subsequently detect unauthorised access in normal cases.

Explanation

The criterion of access control partially substantiates the obligation contained in Art. 32 para. 1 lit. b and para. 2 GDPR to ensure the protection goals of integrity, confidentiality, and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation. This requires an authorisation concept for accessing personal data.

Implementation guidance

The implementation guidance under ISO/IEC 27002 no. 13.2 is applicable.

A appropriate management process for access control should be established that regularly reviews the appropriateness of the need for authorisations, regulates the allocation, updating, control, and withdrawal of authorisations, monitors and updates access policies, reviews password policies, and ensures compliance.

Appropriate security measures against both internal and external attacks should be implemented by the cloud provider to prevent unauthorised access. This includes all standard measures for protecting the cloud host, i.e. host firewalls, network intrusion prevention systems, application protection, antivirus, regular integrity checks of important system files, and host-based intrusion detection systems. The cloud provider should continuously monitor its service for attacks and security incidents in order to detect suspicious activities (e.g. extraction of large amounts of data from multiple clients), attacks, and security incidents in a timely manner and to initiate appropriate and timely responses.

So as to make it more difficult for employees to intentionally interfere with data processing operations, the cloud provider should restrictively assign access authorisation in order to keep the circle of authorised persons small. Employees should only have access to data and data processing operations that they need to complete 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. In order to be able to subsequently track accesses by authorised employees, the cloud provider should log every access.

All relevant security events including security gaps or incidents should be recorded, logged, archived in an audit-compliant manner, and evaluated by the cloud provider. A capable team for security incident handling and troubleshooting should be available at all time so that security incidents can be reported and dealt with promptly.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting the TOMs for access control in the data security concept.

No. 14.5 – Transfer of data and transport encryption (Art. 32 para. 1 lit. b and para. 2 in connection with Art. 5 para. 1 lit. f and para. 2 GDPR)

Criterion

Protection category 1

(1) The cloud provider uses state-of-the-art transport encryption or equally appropriate measures for data transfer processes or requires this through an appropriate configuration of interfaces. The used transport encryption ensures that personal data cannot be read, copied, modified, or deleted during electronic transmission without authorisation. Where the transmission is encrypted, the encryption keys must be securely stored.

(2) As a rule, the cloud provider excludes such acts of unauthorised persons due to technical or organisational errors, including operating errors, of the cloud provider or its employees or due to acts of negligence of the cloud user or third parties. As a rule, the TOMs prevent the negligent disclosure of data to unauthorised persons by the cloud provider and its employees. A minimum level of protection is provided to make intentional interferences more difficult to achieve.

(3) The cloud provider automatically logs 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 the processor and between them.

(5) During the transport of data media, the cloud provider uses TOMs to prevent personal data from being read, copied, modified, or deleted without authorisation. The cloud provider keeps records of the transports.

Protection category 2

(6) The criteria of protection category 1 are fulfilled.

(7) The cloud provider protects the personal data from intentional unauthorised reading, copying, alteration, or deletion and excludes attempts that are to be expected with sufficient certainty. The cloud provider protects against known attack scenarios and, as a rule, (subsequently) detects unauthorised reading, copying, alteration, or deletions.

Explanation

The criterion of transmission and transport control specifies the obligation contained in Art. 32 para.1 lit. b and para. 2 GDPR to ensure the protection goals of integrity, confidentiality, and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation, and to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised admission or disclosure during electronic transmission, transport, or storage on data media.

Implementation guidance

The implementation guidance under ISO/IEC 27018 no. 10.1.1, ISO/IEC 27002 no. 12.4, ISO/IEC 27040:2017-03 no. 6.7.1 and ISO/IEC 27040:2017-03 no. 7.7.1 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting the TOMs for transmission and transport control in the data security concept.

No. 14.6 – Traceability of data processing (Art. 32 para. 1 lit. b and para. 2 in connection with Art. 5 para. 1 lit. c, e, f and para. 2 GDPR)

Criterion

Protection category 1

(1) The cloud provider logs entries, alterations, and erasures of data that occur while performing the contract on the provision of the cloud service or during fulfilment of legal obligations to ensure that data processing can be subsequently verified and traced. The principles of necessity, purpose limitation, and data minimisation must be observed when making logs. Log data must be securely stored.

(2) The cloud provider can, at any time, trace data entries, alterations, and erasures that occur during the intended use of the cloud service by the cloud user or during administrative measures of the cloud provider.

(3) The cloud provider designs the logs of the administrative activities and user activities in such a way that, as a rule, entries, alterations, and erasures can be traced even in the event of technical or organisational errors, including operating errors of the cloud provider or its employees or negligent actions of the cloud user or third parties. The cloud provider provides 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 are fulfilled.

(5) The cloud provider provides protection against expected intentional manipulation of logging instances and against intentional access to or manipulation of logs by unauthorised persons, which excludes expected manipulation attempts with sufficient certainty. These protection

measures include adequate protection against known attack scenarios in particular as well as measures through which manipulation can normally be detected (subsequently).

Explanation

The criterion of traceability partially specifies the obligation contained in Art. 32 para. 1 lit. b and para. 2 GDPR to ensure the protection goals of integrity, confidentiality and availability (SDM 6.2.1 – 6.2.3) of personal data and services in the long term, which requires a high degree of substantiation, and to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised admission or disclosure. To this end, it must be possible to subsequently check and establish whether, and when and by whom and with what effect on content, personal data has been entered, modified, or removed in data processing systems in order to change access rights for the future, if necessary. The secure retention of log data also includes ensuring that the log data can be evaluated.

Because personal data is 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 minimisation and purpose limitation protection goals under Art. 5 para.1 lit. c and b GDPR.

Implementation guidance

The implementation guidance under ISO/IEC 27018 no. 12.4.1, 12.4.2 and ISO/IEC 27002 no. 12.4 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept how it ensures data protection objectives by defining the subject-matter and scope of logging, retention and use of the log data, integrity protection, and deletion of logs.

No. 14.7 – Encrypting stored data (Art. 32 para. 1 lit. a GDPR)

Criterion

Protection category 1 and 2

(1) The cloud provider shall ensure that login data for the use of the cloud service is stored encrypted in such a manner that the provider shall also have no access to this data internally.

(2) The cloud provider shall encrypt personal data that must be stored while performing the contract on the provision of the cloud service or during fulfilment of legal obligations and shall store them in an encrypted manner.

(3) The cloud provider continuously monitors technical developments in encryption and uses encryption procedures that comply with best practice standards.

(4) Implemented encryption procedures shall be replaced by other encryption procedures when they no longer comply with best practice standards.

Explanation

In addition to pseudonymisation, encryption of personal data is explicitly mentioned in Art. 32 para.1 lit. a GDPR as being a security measure to be implemented. The purpose of encryption is to ensure the protection goals of confidentiality and integrity (SDM 6.2.2 and 6.2.2). The threshold above which encryption is required is low, so that, where possible, personal data should be encrypted even when there is a low risk.

Implementation guidance

The state-of-the-art results from current technical standards for cryptographic procedures and their application. The implementation guidance under ISO/IEC 27018 no. 10 and ISO/IEC 27002 no. 10 is applicable.

Encryption keys for encryption should be generated in a secure environment using appropriate encryption key generators. If possible, cryptographic keys should serve only one purpose and should generally

never be stored as a clear key type but should always be encrypted in the system. A redundant and recoverable backup system must be used for storage in order to prevent the loss of a key. Key changes must be carried out on a regular basis. Admission to the encryption key administration system should require separate authentication.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept that the applied encryption procedures correspond to the current technical requirements. The cloud provider shall provide process documentation on how it monitors technical encryption developments and must further keep the suitability of the procedure under review and update it where necessary. In its data security concept, the provider must demonstrate that it has tested the encryption techniques through appropriate technical tests.

No. 14.8 – Separate processing (Art. 5 para.1 lit. b in connection with Art. 24, 25, 32 para. 1 lit. b and para. 2 GDPR)

Criterion

Protection category 1

(1) The cloud provider shall separately process personal data that is processed while performing the contract on the provision of the cloud service or during fulfilment of legal obligations and according to the respective purposes of the processing.

(2) As a rule, data separation must be maintained, even in the event of technical or organisational errors, including operating errors, of the cloud provider or its employees. The cloud provider provides a minimum level of protection to prevent intentional violations of the separation principle.

Protection category 2

(3) The criteria of protection category 1 are fulfilled.

(4) The cloud provider shall exclude intentional violations that are to be expected with sufficient certainty. In the context of data storage, the TOMs needed to achieve this include encryption with individual keys. As a rule, the cloud provider (subsequently) detects intentional violations of the separation rule.

Explanation

The criterion promotes the protection goals of availability, integrity, confidentiality, and unlinkability (SDM 6.2.1 – 6.2.4), thereby also aiming to secure the principle of purpose limitation under Art. 5 para. 1 lit. b GDPR.

Implementation guidance

The implementation guidance under ISO/IEC 27002 no. 12.1.4, 13.1.3 is applicable.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept which TOMs it has taken to separate the data sets from each other according to the purposes of the processing.

No. 15 – Safeguarding the rights of the data subject

No. 15.1 – Information to be provided (Art. 13 in connection with Art. 12 para. 1 and Art. 5 para. 1 lit. a GDPR)

Criterion

The cloud provider shall, through TOMs, ensure that it informs the cloud user, at the time of the collection of its personal data for providing the cloud service and for fulfilling legal obligations,

about the circumstances of the processing and about its rights of the data subject in an intelligible form using clear and plain language. The cloud provider shall inform the cloud user of all required information under Art. 13 para. 1 and 2 GDPR.

Explanation

Where data is obtained directly, the cloud provider is obligated to inform the data subject on the circumstances under Art. 13 GDPR. This criterion promotes the protection goals of transparency and intervenability (SDM 6.2.5 and 6.2.6).

Demonstrating compliance

The cloud provider shall submit the sample of its privacy policy containing the information under Art. 13 para.1 and 2 GDPR, which the cloud user receives when concluding the contract on the provision of the cloud service. If the contract is concluded online, a (test) contract can test whether the cloud provider has provided all information in accordance with Art. 13 para.1 and 2 GDPR.

No. 15.2 – Access to information (Art. 15 in connection with Art. 5 para. 1 lit. a 3rd alt. GDPR)

Criterion

The cloud provider shall, through TOMs, ensure that it grants the cloud user access to the personal data upon request that it processes as the controller for providing the cloud service and for fulfilling legal obligations. The cloud provider shall provide the cloud user with a copy of this data.

Explanation

This criterion promotes the protection goals of transparency and intervenability (SDM 6.2.5 and 6.2.6).

Implementation guidance

Pursuant to Articles 12 para. 3 GDPR, the cloud provider shall provide access to the data subject without undue delay and in any event 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 para. 3 GDPR, the data subject has the right to get a copy of the personal data undergoing processing.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to provide information to the cloud user with undue delay. Whether the information was actually provided can also be verified by means of process documentation.

No. 15.3 – Rectification and completion (Art. 16 in connection with Art. 5 para. 1 lit. d GDPR)

Criterion

The cloud provider shall, through TOMs, allow the cloud user to correct or erase any incomplete or inaccurate personal data relating to the provision of the cloud service on its own. Alternatively, the cloud provider can perform the (legitimate) rectification or erasure.

Explanation

The cloud provider is obligated to rectify inaccurate personal data and complete incomplete personal data of data subjects upon request under Art. 16 GDPR. Rectification pursuant to Art. 16 GDPR promotes the protection goal of intervenability (SDM 6.2.6).

Implementation guidance

The cloud provider is also responsible for the accuracy of data in accordance with Art. 5 para.1 lit. d GDPR, irrespective of the data subject's request, which is why it should set deadlines for the regular review and rectification of data.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which steps it has taken to enable the cloud user to (directly) rectify and complete data or to do so itself.

Whether the data was actually rectified and completed can further be verified by means of process documentation.

No. 15.4 – Erasure (Art. 17para. 1 GDPR)

Criterion

> The cloud provider ensures, through TOMs, that it will erase the cloud user's personal data, which it processes in order to fulfil the provision of the cloud service, without undue delay upon the cloud user's request and on its own initiative if the conditions of Art. 17 para. 1 lit. a, d or e GDPR are met.

Explanation

The criterion promotes the protection goals of intervenability and unlinkability (SDM 6.2.4 and 6.2.6). In particular, there is no obligation to erasure if the cloud provider is obligated to process the data in order to comply with a legal obligation (Art. 17 para. 3 lit. b GDPR).

Implementation guidance

In order to be able to comply with its erasure obligations, the cloud provider should draw up an erasure concept with which it can continuously determine and check its erasure obligations. The erasure concept should include criteria which 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 when statutory permissions have been withdrawn, retention periods, and the legal basis for the storage should therefore be laid down for each data record.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to check and implement the cloud user's request for erasure. Whether the erasure actually took place can also be verified by means of process documentation.

No. 15.5 – Restriction of processing (Art. 18 para. 1 and 3 GDPR)

Criterion

(1) The cloud provider shall ensure, through TOMs, that it may, upon the cloud user's request, restrict the processing of personal data which it carries out for the provision of the cloud service or to fulfil a legal obligation.

(2) The cloud provider shall ensure by using TOMs that it informs the cloud user before the restriction of processing is lifted.

Explanation

Pursuant to Art. 18 para. 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 6.2.6).

Implementation guidance

A restriction of processing may take the form of, for example, a temporary transfer to another processing system or blocking.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which steps it has taken to restrict the processing of data and to inform the cloud user before the restriction of processing is lifted.

No. 15.6 – Notification obligation in the event of rectification, erasure or restriction of processing (Art. 19 in connection with Art. 5 para. 1 lit. a 3rd alt. GDPR)

Criterion

> Insofar as the cloud provider has disclosed to recipients the cloud user's personal data that it processes to provide the cloud service or due to legal obligations, it shall ensure through TOMs that it communicates any rectification or erasure of personal data or restriction of processing to each recipient and informs the cloud user about those recipients if the cloud user requests it.

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 6.2.5 and 6.2.6).

Recipients are, for example, processors that are used to fulfil the contract on the provision of the cloud service.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to comply with its notification obligations and to inform the cloud user, upon request, of the recipients of the disclosure.

No. 16 – Obligation to confidentiality (Art. 5 para.1 lit. a and para. 2 in connection with Art. 24 para. 1 GDPR)

Criterion

> The cloud provider shall only entrust employees with the processing of the cloud user's personal data if, prior to the start of processing, they have been informed about complying with the data protection requirements of the GDPR and are obligated to comply with the requirements.

Explanation

The information about the data protection requirements according to the GDPR and the obligation of the employees to data secrecy promote the principle of fairness and the protection goal of confidentiality (SDM 6.2.3).

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by submitting a sample of employee declarations of commitment or those that are already signed.

No. 17 – Notification of a personal data breach (Art. 33 para. 1, 3 and 5 GDPR)

Criterion

(1) The cloud provider shall notify the supervisory authority without undue delay after having become aware of personal data breaches from processing data while performing the contract on the provision of the cloud service or during fulfilment of legal obligations, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the cloud user.

(2) The cloud provider shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects, and the remedial action taken.

(3) The notification to the competent supervisory authority shall include at least the requirements set out in Art. 33 para. 3 lit. a–d GDPR.

(4) The cloud provider shall determine which factors must be fulfilled so that a risk to the rights and freedoms of the cloud user can be assumed and who is responsible for the notification. The competent employees are 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 so that the supervisory authority can verify the cloud provider's compliance with the requirements of this Article. The criterion promotes the protection goal of integrity and transparency (SDM 6.2.2 and 6.2.5).

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept how it carries out the notification of personal data breaches.

No. 18 – Communication of a personal data breach to the data subject (Art. 34 para. 1 and 2 GDPR)

Criterion

(1) The cloud provider shall inform the cloud user without undue delay of personal data breaches from processing data while performing the contract on the provision of the cloud service or during fulfilment of legal obligations when the personal data breach is likely to result in a high risk to the rights and freedoms of the cloud user.

(2) The notification shall include at least the information under Art. 33 para.3 lit. b, c and d GDPR in clear and plain language.

(3) The cloud provider shall determine which factors must be fulfilled so that a high risk to the rights and freedoms of the cloud user can be assumed and who is responsible for the communication. The competent employees are sufficiently trained to be able to assess violations.

Explanation

A high threat situation, which requires communication to the cloud user in accordance with Art. 34 GDPR, can be assumed, for example, in the event of a loss of bank and credit card information. Such data is often processed for the purpose of performing the contract with the cloud user, so the obligation to communicate data breaches to the cloud user may become relevant.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by documenting in the data security concept how it communicates personal data breaches to the cloud user.

No. 19 – Maintaining records of processing activities (Art. 30 para. 1 GDPR)

Criterion

(1) Cloud providers that employ 250 persons or more shall maintain records of processing activities. The cloud provider shall maintain a record of processing activities, regardless of the number of employees, if the processing is not occasional or is likely to result in a risk to the rights and freedoms of data subjects.

(2) The records of processing activities shall refer to the processing activities that the cloud provider carries out in order to fulfil the provision of the cloud service and legal obligations. The record shall further contain the information listed in Art. 30 para.1 GDPR.

(3) The records of processing activities shall be in writing, including in electronic form. The record shall be made available to the supervisory authority on request

Explanation

The criterion promotes the protection goal of transparency (SDM 6.2.5).

Cloud providers that process data to provide cloud services to the cloud user and employ fewer than 250 persons will also generally have to keep records of processing activities as this data processing takes place regularly and is not occasional, therefore making the exception under Art. 30 para. 5 GDPR not applicable.

If the processing operation is likely to result in a risk to the rights and freedoms of data subjects, or the processing includes special categories of personal data as referred to in Art. 9 GDPR or Art. 10 GDPR, then the processing operation is risky within the meaning of Art. 30 para. 2 GDPR.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by presenting (a representative sample of) the records of processing activities.

No. 20 – Data protection by design and by default

No. 20.1 – Data protection by system design (Art. 25 para. 1 in connection with Art. 5 para.1 and 2 GDPR)

Criterion

Within the framework of the service design, the cloud provider shall ensure through TOMs that only personal data necessary for providing the cloud service is 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 as the processor is only indirectly addressed by Art. 25 GDPR, the cloud provider as the controller is directly addressed. The cloud service technology and organisation must be designed in such a way that they best support the data protection principles of Art. 5 GDPR. The cloud provider must ensure that it only processes personal data that is necessary for the provision of the service to the cloud customer when designing the service. The extent of their processing and their storage period must be limited to what is necessary to achieve the purpose of processing.

Implementation guidance

There are various measures to implement this criterion. They range from the implementation of logins with minimal data for accessing the cloud service to role and authorisation concepts for managing the cloud user's data to erasure concepts for erasing this data. This also includes measures that enable the cloud user to exercise its rights of the data subject as easily as possible because they increase transparency and control possibilities for the cloud user. Examples of measures are the request to access information pursuant to Art. 15 para. 1 GDPR at the push of a button within the service or the online retrieval of data stored on the data subject. The cloud provider should document the considerations that were used as guidelines in selecting the TOMs in order to ensure the data protection principles as this selection may take into account the state of the art, the cost of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

Demonstrating compliance

The cloud provider provides documentation that shows which measures it has taken to implement the data protection principles when designing the cloud service. The documentation also describes the considerations that have been taken to determine the measures.

No. 20.2 – Data protection by default (Art. 25 para. 2 in connection with Art. 5 para. 1 and 2 GDPR)

Criterion

(1) The cloud provider shall, for the initial start-up and use of the cloud service, ensure that, by default, only personal data of the cloud user that is necessary for providing the cloud service is processed.

(2) The cloud provider ensures, by default, that personal data of the cloud user is not made accessible to an indefinite number of natural persons without the cloud user's intervention.

Implementation guidance

There are various measures to implement this criterion. As with No. 20.1, logs with low data protection play a role. Where the use of the cloud service must be logged, so as to detect, for example, misuse or to ensure data security, the default should be chosen in such a way that data is collected and processed anonymously.

Demonstrating compliance

The cloud provider shall document that it has provided protection by default to the cloud user data for the initial start-up and use of the cloud service.

No. 21 – Processing by the cloud provider

Explanatory notes

The data processing necessary to fulfil the contract with the cloud user to provide the cloud service does not have to be personally performed by the cloud provider. Rather, the cloud provider can also outsource data processing (such as invoicing the cloud user for cloud usage) to processors; as such, this outsourcing must also be included in the certification examination.

No. 21.1 – Services governed by a legally binding agreement (Art. 28 para. 3 subpara. 1 sentence 2 GDPR)

Criterion

(1) Where the cloud provider outsources the processing of data needed to provide the cloud service to a processor, it shall conclude a legally binding data processing agreement with the processor.

(2) Through appropriate technical and organisational measures, the cloud provider ensures that data is not processed until after a legally binding data processing agreement has been concluded with the processor.

(3) The legally binding agreement shall be drawn up in writing or in an electronic form.

(4) The cloud provider ensures that the legally binding data processing agreement fulfils the requirements of criteria Nos. 1.2 to 1.6, 1.7 (1), (3)-(4) and 1.8 of Chapter I.

(5) The legally binding data processing agreement includes information on whether the cloud provider or the processor provides for pseudonymisation, anonymisation or encryption procedures.

(6) The legally binding data processing agreement includes information on supporting 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 para. 3 subpara. 1 sentence 2.

The criteria Nos. 1.2 to 1.6, 1.7 (1), (3)-(4) and 1.8 from Chapter I are to be understood in such a way that the cloud provider assumes the function of the cloud user in its role as the controller and the utilised processor assumes the role of the cloud provider.

Demonstrating compliance

The cloud provider shall submit the legally binding data processing agreement(s) with the corresponding specifications that it has concluded with the processor(s).

No. 21.2 – Ensuring proper processing

Criterion

(1) The cloud provider shall ensure that the processor only processes personal data on the cloud provider's documented instructions (Art. 28 para. 3 sentence 2 lit. a, Art. 29 GDPR).

(2) The cloud provider shall ensure that the processor will inform the cloud provider if, in its opinion, an instruction infringes data protection obligations (Art. 28 para. 3 sentence 2 lit. h GDPR).

(3) The cloud provider shall ensure for outsourced processing that the processor guarantees 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, where necessary, adapt the implemented TOMs (Art. 24, 25, 28, 32, 35 in connection with Art. 5 para. 1 lit. f GDPR).

(4) The cloud provider shall ensure that the processor obligates its employees to commit themselves to confidentiality before data processing begins, unless they are subject to a statutory obligation of confidentiality (Art. 28 para. 3 sentence 2 lit. b GDPR).

(5) The cloud provider shall ensure that the processor entrusts only those employees who have the necessary professional knowledge and reliability to carry out processing operations and who are trained in data protection and data security (Art. 28 para. 3 sentence 2 lit. e and f GDPR)

(6) The cloud provider shall ensure that the processor will inform the cloud provider if the data processing place changes unexpectedly (Art. 28 para. 3 sentence 2 lit. a GDPR).

(7) The cloud provider shall ensure that the processor deletes or returns all the data media and all the personal data after the end of the provision of services relating to processing or on the instructions of the cloud provider, and deletes existing copies (Art. 28 para.3 lit. h GDPR).

(8) The cloud provider shall 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 para. 3 lit. e in connection with Chapter III GDPR).

(9) The cloud provider shall ensure that the processor designates a DPO insofar as it is legally obligated to do so (Art. 37–39 GDPR, Sec. 38 BDSG)

(10) The cloud provider shall ensure that the processor maintains a record of processing when it employs more than 250 persons or when the processing is not occasional or when the processing involves risks to the rights and freedoms of the data subjects (Art. 30 para. 2 GDPR).

(11) The cloud provider shall ensure that the processor notifies the cloud provider without undue delay after becoming aware of a personal data breach and its extent (Art. 33 para. 2 and Art. 28 para. 3 lit. f GDPR).

(12) The cloud provider shall ensure that the processor complies with all requirements under the legally binding data processing agreement pursuant to No. 21.1 and fulfils all requirements under these criteria (Art. 24 para. 1 GDPR).

(13) The cloud provider shall ensure that the processor ensures, where it in turn uses sub-processors, that the sub-processors comply with the requirements set out in the criteria No. 10.1–10.5 in Chapter V.

Explanation

Where the cloud provider uses 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 para. 3 subpara. 1 sentence 2 GDPR, but must also ensure that the processor carries out the measures set out in the legally binding agreement and fulfils its other obligations under the General Data Protection Regulation.

Demonstrating compliance

The cloud provider can demonstrate compliance with the requirements by submitting documentation, audit findings, or similar evidence of the processor that convinced the cloud provider so as to assume that the processor fulfils all its obligations under the General Data Protection Regulation and therefore provides for sufficient guarantees under Art. 28 para.1 GDPR.