European Cloud Service
Data Protection Certification

AUDITOR Criteria Catalogue

- Version 1.0 -

Status: 05/06/2024

Related AUDITOR publications:

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

Available online: https://www.trusted-cloud.de

Recommended Citation:

Roßnagel, A., Sunyaev, A., Maier-Reinhardt, N., Müller, J., Lins, S., & Teigeler, H. (2024). AUDITOR Criteria Catalogue – version 1.00. Online available: https://www.trusted-cloud.de

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

Authors

Alexander Roßnagel[a], Ali Sunyaev[b], Natalie Maier-Reinhardt[a], Johannes Müller[a], Sebastian Lins[b], 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] Research group: Critical Information Infrastructures (cii) of the Institute of Applied Informatics and Formal Descriptive Methods (AIFB) at the Karlsruhe Institute of Technology

Table of contents

List of abbreviations and acronyms 4
A. Object and objectives of the AUDITOR Criteria Catalogue 5
1. Addressees and function of the AUDITOR Criteria Catalogue 5
2. TCDP development pursuant to the General Data Protection Regulation 10
B. Structure and use of the AUDITOR Criteria Catalogue 11
1. Elements of the AUDITOR Criteria Catalogue 11
2. Protection categories 11
2.1 The concept of protection categories 11
2.2 The protection categories of the AUDITOR Criteria Catalogue 12
3. Inapplicability of criteria 15
C. Criteria and recommendations for the implementation of Commissioned Data Processing 16
Chapter I: Legally binding Commissioned Data Processing Agreement 16
Chapter II: Rights and obligations of the cloud provider 23
Chapter III: Data protection management system of the cloud provider 56
Chapter IV: Data protection by system design 63
Chapter V: Sub-processing 66
Chapter VI: Processing outside of the EU and EEA 70
D. Criteria and implementation guidance for processing as a controller 78
Chapter VII: The cloud provider as the controller 78
E. References 102

List of abbreviations and acronyms

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

Note on the gender-neutral wording:

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

A. 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). The AUDITOR certification refers to a national data protection certification according to Art. 42 GDPR.[1]

1. Addressees and function of the AUDITOR Criteria Catalogue

The 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 applicable to the contractor (cloud provider) for the processing of personal data. The legal data protection requirements for the client (cloud user) in contrast are not addressed.

AUDITOR object of certification

The object of certification[2] in the AUDITOR certification mechanism comprises 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 certification mechanism mainly focusses on the data processing operations the cloud provider performs as a processor on behalf of a cloud user in accordance with Art. 28 GDPR (hereinafter referred to as “Commissioned Data Processing”). However, also data processing operations are considered, which the cloud provider undertakes in order to enter into and perform the contract with the cloud user for the provision of the cloud service and to fulfil legal obligations. The accompanying document ″Object of Certification" clarifies, describes and illustrates data processing operations in cloud services and lists typical examples (refer to Section B. 2.2).

Data processing operations which the cloud provider undertakes ***as a controller*** in order to enter into and perform the contract with the cloud user for the provision of the cloud service comprise for example:

- to enter into a contract: data, that the provider either needs to implement a technical interface or to decide whether its current interfaces fit to the cloud users technical base for the use of the service. Example data that may be processed include technical data for service provision, such as the browser and device type used, operating system version, unique device identifiers, mobile network information. A name, a phone number, an address, an e-mail-address in order to send an offer to.

- to perform the contract: data, that arise from the processing of the data as agreed upon in the Commissioned Data Processing Agreement in order to receive the service in regard to the conceptual objective of the service as well as usage data[3] in order to invoice accordingly. Example data that may be processed include payment information (e.g., bank account details), usernames and passwords for logging into the cloud service, or user-specific quality indicators (e.g., enabling monitoring or service provision). A name, a phone number, an address, an e-mail-address in order to send a bill to.

- to fulfil legal obligations: data, that are necessary in order to detect anomalies regarding critical infrastructure (e.g., log-in and log-out data for user accounts and IP addresses, location data).

In contrast, the following examples do not constitute data processing operations carried out by a cloud provider as controller in order to enter into or perform a contract with a cloud user:

- data processing operations for market research and analysis (e.g., collecting and analysing data to gain insights into market trends, customer preferences and behaviours),

- data processing operations for marketing purposes (e.g., collecting and processing data to inform about related products),

- data processing operations for (operational) business optimization that are not related to the cloud service (e.g., using data to optimize internal processes and procedures to make cost savings).

[1] The AUDITOR certification is therefore NOT a transfer tool pursuant to Article 46 (2)(f) GDPR.
[2] Note that the term “certification object” corresponds to the term “target of evaluation”.
[3] “Usage Data” are additional personal data such as login/logout data for user accounts, IP addresses, the service modules used, and the extent of use that derive from the use the service.

Once the cloud provider decides to acquire a certification, it will engage in detailed discussions with the certification body to determine the scope of the certification and the concrete data processing operations to be certified. The AUDITOR conformity assessment scheme specifies these processes, and certification bodies are obligated to follow and apply the corresponding processes.[4] Example data processing operations that ***cannot*** be certified under the AUDITOR certification are: (a) data processing operations solely performed as a controller in order to enter into and perform the contract with the cloud user for the provision of the cloud service WITHOUT certifying data processing operations in its role as data processor; (b) data processing operations performing illegal activities; or (c) if the cloud provider's legislation would prevent it from complying with the GDPR principles.

When determining the object of certification, there are three components that cloud providers must consider as addressees 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 not only of technical and automated but also of non-technical organisational components, which are integrated in data protection concepts and data protection management systems. For instance, the certification object covers support or maintenance activities, in case personal data is processed. 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 taken into account to the complete extent. This means that interfaces of the certified cloud services with other services must also be taken into account so as to identify data flows from which data protection risks may arise. Further information about the AUDITOR object of certification and example data processing operations can be found in the accompanying document ″Object of Certification".

Cloud providers as addressees

A *cloud provider* within the meaning of this catalogue is any company in the private sector providing a cloud service on the market and seeking certification pursuant to 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 processors* of data processing operations (s. Chapter C). Cloud providers can be both B2B[5] and B2C[6] providers. What is important is that they are involved as the processor of the data being processed in the cloud ("**content or application data**"[7]) and not as the controller, and they seek certification of the conformity of their data processing operations with data protection requirements. 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 controllers* of data processing operations. Cloud providers are also addressed as the controllers of data processing operations, which are necessary to enter into and perform the contract for the provision of the cloud service with the cloud user. If the cloud service is offered in the B2C segment, the cloud user

[4] Among others, a certification body must refuse to carry out a particular certification if (a) it lacks the competence or capability for the certification activities it is required to perform, (b) it lacks the resources to carry out all selection and determination activities; or (c) its impartiality is compromised. A certification body further can reject cloud provider's request for certification if the cloud provider is involved in illegal activities, the cloud provider has repeatedly violated the AUDITOR certification criteria, or there is evidence of similar problems relating to the cloud provider. The certification body is requested to perform selection processes that are free from arbitrariness in the assessment and document their decisions in a transparent manner.

[5] Business to Business (B2B) means, that the client is either a legal or a natural person, processing personal data in line of his business. A 'business' means any natural person or legal person who or that, in contracts, is acting for purposes which are **inside** his trade, business or profession.

[6] Business to Consumer (B2C) means, that the client is a natural and private person, therefore is not processing personal data in line of his business. Please also refer to "Cloud users as beneficiaries" (p. 6) in regard to the cloud user as a natural person falling under the "household exemption". A 'consumer' means any natural person who, in contracts, is acting for purposes which are **outside** his trade, business or profession. It must, however, be noted, that a consumer does not automatically fall under the so-called "household-exemption" according to Art. 2 (2) lit.c GDPR. This exemption is reserved for the non-applicability of the processing of personal data by a natural person in the course of a purely personal or household activity. A consumer´s data processing can thus either fall or not fall under this exemption with the consequence, that its data processing is either privileged or not. In case of the latter the consumer is to be treated as a controller.

[7] Content data are itself carrying information about a data subject whereas application data are information about a data subject derived from the use of a software application, e.g. content data in a document would be the meaning in words whereas application data would stem from the software-program being used to be able to read the documents content.

often represents the data subject, whose data are necessary to provide the cloud service, so that the cloud provider must fulfil its data protection obligations towards the cloud user (e.g. obligations to inform).

In the B2B segment, it must be noted that data from legal persons such as names or addresses according to Recital 14 are excluded from the scope of the General Data Protection Regulation. However, this does not apply if the data of the legal person have a close personal or economic link to a natural person, e.g. in the case of a limited liability sole proprietorship. In this case, personal data are also present, and the General Data Protection Regulation is applicable.

Where the cloud user concludes a contract with the cloud provider for the provision and use of cloud services, the cloud provider will be obligated to process personal data foremost being subject to 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 generally free to choose the processing purpose and the matching legal basis under Art. 6 (1) subpara. 1 sent. 1 lit. a) to f) GDPR and Art. 5 (1) lit. b) in conjunction with Art. 6(4) GDPR does not have a strict purpose limitation but provides only for the reconcilability with the purpose, the AUDITOR certification exclusively examines the data processing of the cloud provider in its role as the controller, which 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, which are performed by the cloud provider in order to provide the cloud service to the cloud user so as to enable the use of the service and invoice the user accordingly for the service.

In order to enter into and perform the contract with the cloud user for the use of the cloud service, the cloud provider decides which personal data it collects and processes. Usually, data are processed such as names, addresses, payment information such as bank account information, phone numbers, user names, and passwords for logging into the cloud service. They can be grouped under the term **"master data"**. Especially in the B2B segment, in addition to the data of the cloud user, data of other data subjects like employees of the cloud user may be required for the conclusion and performance of the contract with the cloud user for the use of the cloud service. For example, names and contact data of employees of the cloud user, which are to act as the contact persons for the cloud provider, can be processed. Since the cloud provider does not conclude the contract for the cloud use with the employee, Art. 6 (1) subpara. 1 lit. b) GDPR does not legitimise the processing of employee data. Instead, the cloud provider can refer to Art. 6 (1) subpara. 1 sent. 1 lit. f) GDPR and its legitimate interests in data processing for as long as the data are necessary for the conclusion and performance of the contract with the cloud user.

To enable the cloud user to use the cloud service with the corresponding invoicing of the service to the user, the cloud provider must process additional personal data such as login/logout data for user accounts, IP addresses, the service modules used, and the extent of use. These data can be grouped under the term **"usage data"**[8]. The processing of telemetry and diagnostic data is also grouped under this term, as long as the data are necessary for the performance of the contract with the cloud user.

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

A cloud provider should refrain from applying for certification if it is aware that its legislation would prevent it from complying with the GDPR principles enshrined in this certification scheme.

Cloud users as beneficiaries

A *cloud* user within the meaning of this catalogue is any natural person or legal person in the private sector, 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 the purposes and means of this processing, and who makes the decision on outsourcing this processing to a cloud provider.

Since a cloud user can be a legal person it is to be noted, that its decision to outsource data processing to a cloud provider, generally means, that personal data of natural persons that work for it will be, in dependence to the service chosen, likely to be processed by the cloud provider too, in order to perform the contract with the cloud user. As a consequence, a cloud provider processing as a controller (Chapter D.) will process data of the cloud user, with whom it has entered into a contract and those persons, that work for the cloud user, in order to allow the performance of the contract. As a further consequence this means, that the term "cloud user" in Chapter D. will entail legal entities, natural persons and data subjects, to whom the cloud provider´s processing as a controller is to be fully GDPR-compliant.

[8] "Usage Data" are additional personal data such as login/logout data for user accounts, IP addresses, the service modules used, and the extent of use that derive from the use the service.

Since a cloud user can also be a natural person, its processing may be privileged.

The processing of personal data by the cloud user as a natural person may fall under Art. 2 para. 2 lit. c GDPR, the so called “household-exemption”, when processing “in the course of a purely personal or household activity”. To those processing the GDPR does not apply. As processing of personal data under the household-exemption is rather limited, somewhat fluent[9] and granted very restrictively by the supervisory authorities the basic concept of the cloud provider as the processor still applies in that situation.[10] Nevertheless, the GDPR would still apply to the cloud provider acting as the processor and providing the means for such processing.[11]

A processing of a natural person “in the course of a purely personal or household activity” will have to be established e.g. with the help of the following general criteria[12]:

- In order for the exemption to apply, a 'natural person' must process. Processing by legal entities, irrespectively of their form (including NGOs, Foundations, Trusts and alike), is not covered by the exemption
- A “personal or household activity” refers to the “private”-life of the natural person processing. The 'private'- from the 'non-private'-life can be drawn out from the existing case-law:
    - “private” must be interpreted as covering only activities that are carried out in the context of the private or family life of individuals: “*an activity cannot be regarded as being purely personal or domestic where its purpose is to make the data **collected accessible to an unrestricted number of people** or where that activity extends, even partially, to a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner*”[13]
    - Neither the publication of personal data on a blogging site made available to an unlimited number of people could therefore be subject to the household exemption[14] nor could a camera system installed on a family home for the purposes of protecting the property insofar as it also records a public space[15]
- The 'private'- from the 'non-private'-life can also be drawn out from recital 18 GDPR as
    - personal correspondence,
    - keeping of addresses, or
    - social networking and online activity as long as they are purely personal or a household activity, which indicates, that sharing of information with ***a limited number of close friends*** can still be seen as a purely personal activity.

Establishing, whether a natural person falls under the household exemption, will in practice not be conducted by cloud providers, since they need to offer a service, that is fully GDPR-compatible on the basis of the rule, meaning not based on the assumption of the exemption to it. Since the cloud provider´s service therefore needs to be compliant with this Criteria Catalogue, as it is exclusively addressed to it, not to the data subject, it still could be interested to know, how to establish, whether in practice the household exemption applies. There are three basic factors, that could be taken into regard, when establishing the application of the household exemption:[16]

- assess the space of the processing. Activities that take place in a private space can be considered 'personal'. Public places or generally available websites are excluded from the application of the household exemption.
- assess the social aspect of the processing. One needs to review the relationship between the natural person who carries out the processing and the data subjects and the extent of the group of subjects who have access to the personal data.

[9] The limit of a processing of personal data as "purely personal or household activity" is likely to be easily exceeded leading to the consequence that GDPR´s privileged treatment of the cloud user ends. It therefore must then comply with its obligations as a controller within the meaning of Art. 4 no. 7 GDPR.
[10] I.e. the cloud provider has to fulfil all requirements as foreseen in part “C. Criteria and recommendations for the implementation of Commissioned Data Processing”.
[11] Recital 18 GDPR.
[12] https://gdprhub.eu/Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity. See also margin number 11-14 of “EDPB-Guidelines 3/2019 on processing of personal data through video devices”.
[13] CJEU - C-25/17 - Jehovan todistajat, ECLI:EU:C:2018:551.
[14] CJEU - C-101/01 - Bodil Lindqvist, ECLI:EU:C:2003:596.
[15] CJEU- C-212/13 - František Ryneš, ECLI:EU:C:2014:2428.
[16] https://gdprhub.eu/Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity.

- determine the purpose pursued by the controller. According to Recital 18, these activities must have no connection with anything 'professional' or 'economic'. Consequently, if the activities pursue such purposes, the exemption will not apply.

Whereas the applicability of the household exemption does not affect the obligations of the cloud provider as processor, the cloud user does not fall under the obligations of the GDPR. Bearing this in mind, the requirements listed in Art. 28 (3) GDPR will be distinguished as follows:

As far as Art. 28 (3) GDPR contains obligations directly aimed at the processor, these obligations have to be fulfilled by the processor. In this respect the applicability of the household exemption does not cause any need to changes. This applies for the requirements listed in Art. 28 (3) (a), (b), (c), (d) and (h) GDPR.

As far as Art. 28 (3) GDPR, however, ties in with obligations according to the GDPR to which a controller is subject and from which the processor's obligation to assist the controller is derived, the applicability of the household exemption must be taken in account. Due to the household exemption the cloud user is not subject to the obligations attributed to a controller (for instance: Art. 12 ff. GDPR, Art. 33 and 34 GDPR, Art. 35 and Art. 36 GDPR). Thus, there is no "connecting factor" for the processors' obligation to assist the controller. This applies for the requirements listed in Art. 28 (3) (e), (f) and (g) GDPR.

A respective note is included below under the respective criteria. Before outsourcing its processing to a cloud provider, the cloud user should examine whether Commissioned Data Processing is permitted for its processing operations or if there are special requirements (e.g. professional secrecy obligations of lawyers [§§ 43a para. 2; 43e Federal Code for Lawyers] and physicians [§ 9 of the Medical Association's (model-) professional code of conduct] as protected by § 203 German Criminal Code) outside of the GDPR. It should be noted, however, that the AUDITOR certification is aimed at neither cloud users nor cloud providers in the public sector.

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 complies with data protection requirements. The scope of application of the data protection certification pursuant to AUDITOR is the processing of personal data on commission (Commissioned Data Processing) in accordance with Art. 28 GDPR by a cloud provider. In this case, the cloud user of the service, being a client in accordance with Art. 28(1) GDPR, must satisfy itself that the cloud provider provides sufficient guarantees that appropriate technical and organisational measures (TOM) are implemented in such a manner that the processing meets the requirements of the General Data Protection Regulation and that the rights of data subjects are protected. Proof of sufficient guarantees is simplified if the cloud provider, as the contractor, presents a certificate that confirms the fulfilment of the legal requirements. A certificate may be used in accordance with Art. 28 (5) GDPR as one factor to prove sufficient guarantees. For the use of cloud services that are normally 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.

Cloud users should, irrespective of the presence of the AUDITOR certification, nonetheless perform an assessment of the legislation of the host country before transferring data to the non-EU GDPR certified processor. In case the legislation does not provide for the appropriate level of protection, supplementary measures should be put in place.

Personal data as information to be protected

Personal data according to the legal definition under Art. 4 (1) GDPR are all data that relate to an identified or identifiable natural person. In a cloud context, this could be, for instance, the cloud user's application data if it enables the respective data processor to identify a natural person or make a natural person identifiable. In accordance with Art. 28 (3) subpara. 1 sent. 1 GDPR, the cloud users and cloud providers must determine, in a legally binding Commissioned Data Processing Agreement[17], which types of personal data are to be processed by the processor, who shall be 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 that apply to the cloud provider in its role as processor. Data processing operations for which the cloud provider does not merely act bound by instructions but where it determines the purpose and means of processing personal data as the controller are considered in the context of the AUDITOR certification only where the processing of personal data of the cloud user or other data subjects such as the employees of the cloud user is concerned that is required for the provision of the cloud service and enabling its use with accordant invoicing, and where the data processing serves for the fulfilment of legal obligations applicable to the cloud provider.

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, the specific designs, as well as the individual

[17] "Commissioned Data Processing Agreement" is the contract between the cloud service provider and the client containing the specifica of the data processing in accordance with the requirements of Art. 28 para. 3 GDPR.

processing agreements with the cloud users. It is therefore up to the cloud user and cloud provider to determine rules for distributing responsibilities.

The rules must reflect the actual distribution of possibilities to take influence on the data processing between the parties. The greater the cloud provider's possibilities of influencing data processing, the more likely it will be viewed as the controller. According to Art. 4 no. 7 GDPR, the controller is the body determining the purposes and means of data processing. The cloud provider is a processor if it carries out the Commissioned Data Processing in accordance with the instructions and does not pursue its own purposes with the data to be processed. However, the cloud provider often has certain decision-making powers regarding the choice of technical and organisational means. Insofar as such means are suitable to achieve the purpose of the processing and provided it informs the cloud user about this before their use and the cloud user agrees to their use, the cloud provider remains a processor.

As a rule of thumb, the cloud user must regularly be regarded as the controller of the personal data, which is transferred to the cloud by the cloud user or persons associated with the user. This concerns the cloud user's content and application data. The cloud provider is responsible for the data processing operations that it operates so as to perform the cloud service and enable its use and to invoice the user accordingly. This usually relates to master data and usage data.

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 subcontracted processors (sub-processors) for the provision of services, provided that the cloud user agrees thereto. 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 must not result in the provisions of the General Data Protection Regulation being disregarded in the service chain. Instead, the cloud provider as the main processor must ensure 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 use platforms or infrastructures not owned by the provider or if the processor involves other sub-processors, the certificate may apply exclusively to the data processing operations, which are within the responsibility of the respective processor. However, the processor must convince itself that these third-party platforms, infrastructures, and sub-processors used by it also comply with the data protection regulations applicable to them and that it may use exclusively such and no others for the provision of its cloud service.

A cloud provider may therefore only select those sub-processors which, in accordance with Art.28 (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 also provide the required suitable guarantees, e.g. in the form of a data protection certificate or by compliance with approved codes of conduct pursuant to Art. 40 GDPR. Chapter V of this Criteria Catalogue regulates subcontracted processing in particular.

2. TCDP development pursuant to the General Data Protection Regulation

The certification pursuant to the old Federal Data Protection Act was examined in the pilot project "Data Protection Certification for Cloud Services" by the Trusted Cloud Data Protection Profile (TCDP), which 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, not the requirements of the General Data Protection Regulation could be taken into account when developing the certification criteria according to TCDP, the TCDP criteria must be adapted to the new regulations as of the application of the General Data Protection Regulation on 25 May 2018. This is done in the AUDITOR Criteria Catalogue.

The AUDITOR Criteria Catalogue focuses on all relevant regulations 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 “proof”. The "criteria" describe the normative requirements to 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” serve as guidance using typical examples for understanding and implementing the criteria; however, they are not binding. Implementation guidance is also not conclusive but they describe central implementations of the criteria. The implementation guidance is based on existing industry standards, norms and best practices as appropriate. For example, with regard to the criteria under no. 2 for the assurance of data security, in particular, it is referred to ISO/IEC 27002 and BSI C5 and corresponding text sections are cited. Moreover, for each criterion there is a “*proof*” section included, which provides the answer to the question of how it can be proven that the criteria are fulfilled in the specific certification mechanism. Similar to the implementation guidance, this part serves as guidance and provides informative help that is intended to support cloud providers, certification bodies, auditors, and other interested parties in assessing compliance with the criteria. For example, the submission of documentation for testing by the certification body is suggested, or an on-site audit by the certification body is required as proof of the implementation of documented measures. There is no obligation to demonstrate compliance with the requirements by performing the specific proof guidance. The accredited AUDITOR conformity assessment programme determines how each criterion is to be tested for the certification.

The Criteria Catalogue differentiates between criteria, explanations, implementation guidance, and proof for the processing of application data (Chapter C), and for the processing of master data, and usage data for which a cloud provider is responsible (Chapter D).

2. Protection categories

Requirements for TOMs of the cloud service are differentiated by protection categories. At the same time, the AUDITOR Criteria Catalogue is orientated on the TCDP protection categories concept, it also considers the classifications of the need for protection according to the Standard Data Protection Model (SDM). The accompanying document "Protection Categories Concept" summarises the conception and differentiation of the protection categories in detail.

2.1 The concept of protection categories

The protection categories concept is based on the risk of data processing for the fundamental rights and freedoms of natural persons. In addition, pursuant to Art. 24, 25 and 32 GDPR, the selection of TOMs 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 arising from the processing of personal data to the rights and freedoms of natural persons ahead of time. In another step, it must be assessed whether the processing might lead to material or immaterial damage, particularly if it might lead to discrimination, identity theft or fraud, financial loss, damage to reputation, loss of the confidentiality of the personal data protected by professional secrecy, unauthorised reversal of pseudonymity, or other significant economic or social disadvantages, if the data subject is deprived of his rights and freedoms, or prevented from controlling his personal data.

In accordance with Recital 76 sentence 1 GDPR, the controller must assess 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 must assess this risk according to the respective utilisation context of the processed personal data on the basis of an objective standard. Pursuant to Recital 76 sentence 2, it must determine at the same time whether the data processing involves a risk or a high risk. These risk classifications are implemented in the AUDITOR concept of protection categories.

Conversely, the cloud provider must indicate 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 assigned to each individual data protection operation but to the cloud service as such.

The objective of the protection categories concept is to simplify the individual standard of the General Data Protection Regulation – the TOM requirements are based on the protection requirement of the respective data processing – by attribution to protection categories. The protection categories therefore have a dual function: they describe the protection requirement of the data processing operations and the TOM requirements. To make the different functions clear, the protection categories concept distinguishes between categories of protection requirements on the one hand and categories of protection needs on the other hand.

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

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

The differentiation of protection needs categories of, and protection requirements categories correspond to the roles and responsibilities of cloud users as controllers and cloud providers as processors. As part of the certification process, the cloud provider claims a specific category of protection requirements for each service on the basis of the assessment 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 client, however, the cloud user has the task of determining the required protection needs for its data processing, by selecting a protection needs category. 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 required for the performance of the cloud service for use by the cloud user, the provider shall determine the protection need as well as the protection requirements for the data processing because both fall within the provider's responsibility.

2.2 The protection categories of the AUDITOR Criteria Catalogue

The AUDITOR Criteria Catalogue is based on the differentiation between three protection categories (I, II, III) for which the respective protection needs (protection needs categories) and protection requirements (protection requirements categories) are described.

Data processing operations with an extremely high protection need (above protection needs category 3) are also not considered in the Protection Categories Concept nor in 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 a critical informative value concerning the personal identity or circumstances of the data subject or they can support or result in such or they are otherwise of considerable importance as relates to the circumstances of the data subject and if 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.

This list of examples of data with extremely high protection needs is not exhaustive:

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

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

a) Assessment of the protection needs category

The cloud user is responsible for assessing the protection needs. The protection needs are assessed 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 according to the categories of protection needs. Steps 2 and 3 are not explained any further in the AUDITOR Criteria Catalogue, because they concern the cloud user and not the certification of the cloud provider as such. For further information, please refer to the accompanying document "Protection Categories Concept".

It must be noted, however, that the cloud provider is the data controller in data processing for the performance of the contract with the cloud user and also with regard to the fulfilment of legal duties, which is why it must determine the protection need of this data processing too.

Protection needs categories according to the data type (abstract protection need – step 1)

Firstly, the abstract protection need of the data to be processed is determined according to the data type. This is merely the starting point serves only for the initial classification of the data. After all, the protection need of data cannot be determined in an abstract manner but it rather depends on the context of its respective use.

Data types with a normal protection need (protection needs category 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.

Protection needs category 1 includes all data processing operations containing, generating, supporting or permitting statements about the personal or material circumstances of the data subject based on the data that are entered and the specific processing of this data. 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 list of examples of data (without processing context, if not included in protection needs category 2 or 3):

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

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

Data processing operations, which are capable of providing or sustaining informative value about the personality or life of the data subject or which could lead to such information or otherwise be relevant regarding the data subject's circumstances, based on the data used or the specific processing of these data. The unauthorised processing of such data can result in damage to the social status or economic circumstances of the data subject ("reputation"). In addition, data identified as requiring a particular measure of protection by the legislator in Art. 9 (1) GDPR must be presumed to have a high need for protection.

Non-exhaustive list of examples of data (without processing context, if not included in protection needs category 3):

- Name, address of a contracting party;
- Date of birth;
- Marital status;
- Family relations and acquaintances;
- Data on business and contractual relationships;
- Context relating to a contractual partner (e.g. object 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 with potential effects on the standing/reputation of a data subject;
- Data about the protected internal 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, etc.);X
- Data relating to time in employment

- 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 reviews 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);X
- (Exact) location of a person;
- Financial data of 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. The determination of the protection need requires an objective assessment in which the extent of the risk of the data processing is identified. If the cloud user has no knowledge of the subjective protection need of the parties communicating (e.g. general collaboration service with data storage, video conferencing and email function) or if it offers services for communication that has special protection needs (e.g. conferencing services for lawyers and clients, here: protection category 3), it may assume that protection needs category 2 applies.

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

Data processing operations, which are capable of providing or sustaining considerable informative value about the personality or the circumstances of a data subject or which could lead to such information or which are otherwise of considerable significance to the data subject's circumstances based on the data used or the specific processing of these data. The unauthorised processing of such data may result in considerable disadvantages for the data subject regarding its social status and its financial circumstances ("livelihood").

Explanatory note: Data types in this sense also include data majorities, in particular linked data (e.g. personality profiles) from which new informative content results.

Non-exhaustive list of examples of data with very high protection need:

- Data that are subject to professional, business, telecommunications or client secrecy (e.g. patient data, client data);
- Data the knowledge of which may cause significant specific harm to the data subject or a third party (e.g. personal identification number, transaction number in online banking);
- Debts;
- Particularly sensitive social data;
- Seizures;
- HR management data such as employment evaluations, professional career, etc. if not included in protection needs category 2;
- Data of previous convictions and circumstances relating 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 disclosure 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 appropriate TOMs to protect the rights and freedoms of data subjects adequately with regard to the risks of service identified in the protection needs category.

Category of protection requirements 1

The cloud provider must take risk-appropriate TOMs to ensure data minimisation, availability, integrity and confidentiality, unlinkability, transparency, and intervenability of personal data (see protection goals under SDM). For data 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.

The TOMs must be appropriate to regularly prevent such processes that are caused by technical or organisational errors, including operating errors of the cloud provider or its employees, or by negligent acts 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 TOM 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 SDM). For data 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. 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 TOM of the categories of protection requirements 1 and 2, the cloud provider must achieve risk-appropriate TOM to protect the data, in particular against destruction, loss, alteration, unauthorised access, and unauthorised disclosure.

The measures must be appropriate to regularly prevent such processes that are caused by technical or organisational errors, including operating errors of the cloud provider or its employees, or by negligent or intentional acts of third parties with sufficient certainty. 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 the documentation of responsibilities and, insofar as is applicable, involving sub-processors in the data processing operations to be certified. Generally, not all criteria of the AUDITOR Criteria Catalogue will be applicable to every object of certification. 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 how an accredited certification body determines the inapplicability of criteria. It requests that inapplicable criteria are documented and for each criterion a detailed justification (i.e. why it is not applicable to the specific certification object) must be documented as well. The certification body must ensure that the assessment of non-applicability relates to the specifics of a specific certification object (i.e. the cloud service to be certified and its processing operations) and that same decision regarding non-applicability is made for comparable certification processes and circumstances in order to prevent the possibility of arbitrariness. In particular, a free or arbitrary selection of criteria and the establishment of non-applicability should be prevented. If the certification body has doubts about the non-applicability of a criterion, the certification body attempts to resolve the ambiguities. For this purpose, further documents and explanations can be requested from the cloud provider, or determination methods can be used by the certification body. In case the certification body awards the certification to the cloud service provider, the body provides, among others, a public summary report of the result of the certification. The public summary report documents the use of the certification object in the area of application and the use cases in a transparent and comprehensible manner, so that individuals can comprehend in a reasonable time what is guaranteed when using the certification object in the sense of data protection law.

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 obligated to assist the cloud user in providing information according to the criterion no. 6.2. However, the criterion does not apply to the cloud provider’s data processing operations, thereby exempting the cloud provider from providing information if the cloud user is responsible for the data in question and determines the applications and files (for example, in the case of infrastructure-as-a-service). 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 does not apply to the cloud provider. The cloud provider,

however, must assure itself that the sub-processors comply with the data protection regulations applicable to them (see No. 10.4) and that they consequently comply with criterion No. 2.3.

Furthermore, criteria are not applicable if the cloud provider does not perform the tasks described in the criteria. If, for example, the cloud provider does not involve sub-processors or if no data are processed outside of the EU or the EEA, the criteria in Chapters V and VI are not applicable.

C. Criteria and recommendations for the implementation of Commissioned Data Processing

Chapter I: Legally binding Commissioned Data Processing Agreement

Explanation

The cloud provider must ensure that the services are provided for the cloud user on the basis of a legally binding agreement[18] fulfilling the legal requirements for Commissioned Data Processing under the General Data Protection Regulation. The legal requirements for this agreement are specified by the following criteria under numbers 1.1 to 1.8.

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

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

Criterion

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

(2) The legally binding Commissioned Data Processing Agreement must be documented in writing or in an electronic form.[19]

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

Explanation

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

Implementation guidance

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

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

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

Proof

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

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

As part of the certification process, the cloud provider should submit the template legally binding Commissioned Data Processing Agreement and all or a representative sample of legally binding agreements that it concludes with the cloud users. In addition, it can use suitable documentation (e.g. process documentation, function documentation, or log files) to prove that TOMs have been implemented, which ensure that the service is used only after the legally binding Commissioned Data Processing Agreement has been concluded (e.g. in regard to an agreement or registration process with potential cloud users). By simulating a corresponding agreement or registration process on a test basis, the cloud provider can demonstrate that the concepts specified in the documentation have also been implemented in the cloud service.

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

Criterion

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

(2) The legally binding Commissioned Data Processing Agreement must specify the duration of the processing by a start and an end point or refer to an indefinite period of use.

Implementation guidance

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

Reference is made to the implementation guidance for the transparent system description in BSI C5 Section 3.4.4 and BC-01 to BC-06.

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

Proof

The cloud provider can demonstrate compliance with the requirements by submitting documentation for the legally binding Commissioned Data Processing Agreement with this information (e.g. sample contracts, contract templates or contract instances). By means of a test use of the service (in particular, insight of whether content is displayed when registering for the use of the service), the cloud provider can demonstrate that it has implemented a procedure according to which a legally binding Commissioned Data Processing Agreement containing these regulations will be concluded.

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

Criterion

The legally binding Commissioned Data Processing Agreement must determine the nature and purpose of the intended data processing in the order, the type of data processed and the categories of data subjects.

Implementation guidance

It is permissible that the cloud provider offers a generalized description of the nature, scope and purposes of data processing. Nevertheless, the information in the Commissioned Data Processing Agreement should be tailored to the specific processing, such as stating predefined types of data, categories of data subjects, or typical functions to achieve certain data processing purposes. The description should be precise enough to allow cloud users to make an informed decision which cloud service to use. The cloud user may be able to enter the information relevant for the cloud user's specific case.

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

Reference is made to the implementation guidance in the SDM module 41 "Plan and specify" and 42 "Documentation".

Proof

The cloud provider can demonstrate compliance with the requirements by submitting documentation for the legally binding Commissioned Data Processing Agreement with this information (e.g. sample contracts, contract templates or contract instances). By means of a test use of the service (in particular insight of whether content is displayed during registration for the use of the service), the cloud provider can demonstrate that it has implemented a procedure according to which the legally binding Commissioned Data Processing Agreement containing these regulations will be concluded.

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

Criterion

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

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

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

(4) If a legally binding Commissioned Data Processing Agreement is entered into within the framework of standardised bulk transactions on the basis of general terms and conditions, the cloud provider must - before a legally binding Commissioned Data Processing Agreement is entered into - name in its service description, in as much detail as possible, the services it can technically perform in a manner that is comprehensible from a cloud user's perspective so as to enable a selection in accordance with Art. 28 (1) GDPR. In the legally binding Commissioned Data Processing Agreement, the cloud provider must undertake to inform the cloud user if, in its opinion, an instruction of the cloud user violates data protection provisions.

Explanation

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

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

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

Implementation guidance

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

The technically feasible services and the cloud user's authorities to issue instruction should be listed in the legally binding Commissioned Data Processing Agreement of the cloud provider. The legally binding Commissioned Data Processing Agreement should describe users' rights to instruct the cloud provider, including the rights to change, amend, and withdraw instructions. The agreement should not restrict cloud users' right to issue instructions in order to keep the processing GDPR-compliant. Cloud users may issue instructions manually or by using automated procedures and functions (e.g. API requests, software commands, or clicking on cloud services' functions). On the basis of the cloud provider's service description (unilaterally pre-defined in bulk transactions), the potential cloud users should receive information on their selection pursuant to Art. 28 (1) GDPR.

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

Reference is made to the implementation guidance for the transparent system description in BSI C5 Section 3.4.4 and PSS-01.

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

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

Proof

The cloud provider can demonstrate compliance with the requirements by disclosing corresponding regulations regarding legally binding Commissioned Data Processing Agreement s for issuing instructions, informing the cloud user about instructions that are contrary to law, processing that is not bound by instructions based on legal obligations under Union or Member State law and for establishing appropriate safeguards for a data transfer to third countries or to international organisations (e.g. provision of sample contracts, contract templates or contract instances). Where appropriate, it can present existing documentation of individual instructions. By means of a test use of the service (in particular, disclosure of whether content is displayed during registration for the use of the service), the cloud provider can prove that it has implemented a procedure according to which the legally binding Commissioned Data Processing Agreement containing these regulations will be concluded.

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

Criterion

(1) In the legally binding Commissioned Data Processing Agreement, it must be determined whether the cloud provider processes the data of the cloud user within the EU/EEA or in a third country.[20]

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

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

(4) The legally binding Commissioned Data Processing Agreement must provide that the cloud user must be able to effectively object to changes in the place of processing, if they have a substantial effect[21] on the previous assessments carried out.

Explanation

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

Implementation guidance

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

Exclusive data processing in the EU or the EEA does not always prevent personal data from being automatically withdrawn from access by public authorities of third countries. For example, the Cloud Act can also require cloud providers based in the EU, which are affiliated with a US parent company and process personal data exclusively in the EU or in the EEA, to disclose this personal data stored in the EU or in the EEA to US authorities.

Similar regulations may also apply in other national laws of third countries. Choosing cloud providers is not prohibited per se, but cloud users and cloud providers must find solutions to effectively protect personal data from access by the public authorities of the third country concerned. One possibility is, e.g. hiring a trustee who is subject exclusively to European law and who has exclusive access to the outsourced data of the cloud user. As a result of the trust agreement, the personal data are neither owned nor under the control of the cloud provider and could

[20] This also includes the location of processing activities conducted by sub-processors when the cloud provider engages another processor for carrying out specific processing activities on behalf of the controller.
[21] A substantial effect on the previous assessments carried out shall be deemed to be given if the new place of processing would involve a data transfer outside the EU/EEA.

consequently not be released to US authorities. For some cloud services, encryption can also be a solution. See the use cases in no. 11.1 and the other explanations there.

Reference is made to the implementation guidance in BSI C5 BC-01 and PSS-12.

Proof

The cloud provider can demonstrate compliance with the requirements by submitting appropriate documentation (e.g. sample contracts, contract templates or contract instances). By means of a test use of the service (in particular, insight of whether content is displayed during registration for the service use), the cloud provider can demonstrate that the place of data processing (within the EU or the EAA or the specific third country) and the obligation to report changes of place are communicated to the cloud user in a suitable manner.

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

Criterion

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

Explanation

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

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

Implementation guidance

Reference is made to the implementation guidance in BSI C5 HR-05 and HR-06.

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

Proof

The cloud provider can demonstrate compliance with the requirements by submitting appropriate documentation (e.g. sample contracts, contract templates or contract instances) verifying that it undertakes to make the persons authorised to process personal data subject to confidentiality obligations before they begin with the data processing activities, if they are not already subject to an appropriate, comparable legal obligation of confidentiality. By means of a test use of the service (in particular, insight of whether content is displayed during the registration for the service use), the cloud provider can demonstrate that it has implemented a procedure according to which the legally binding Commissioned Data Processing Agreement containing these regulations is concluded.

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

Criterion

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

(2) The legally binding Commissioned Data Processing Agreement must include the statement of whether the cloud provider or cloud user carries out pseudonymisation, anonymisation or encryption (no. 2.7, no. 2.8 and no. 2.9) of the personal data. The statement should clarify whether these mechanisms are also effective towards the staff of the cloud provider that may have access to the personal data.

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

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

(5) The procedures and TOMs, which are to assist the cloud user in the fulfilment of data subjects' rights in accordance with no. 6, in carrying out a data protection impact assessment in accordance with no. 7, and in fulfilling the reporting obligation in the event of data protection breaches in accordance with no. 8.2, must be defined in the legally binding Commissioned Data Processing Agreement.[22]

Implementation guidance

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

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

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

Since the cloud user has a right to object to changes in subcontracted processing (no. 10.3), the legally binding Commissioned Data Processing Agreement should address the prerequisites and consequences of an objection, such e.g. as whether the cloud user may terminate the legally binding Commissioned Data Processing Agreement upon objection. The cloud user´s right to object to changes in subcontracted processing must not be devalued in practice (see no. 10.1[1]).

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

Reference is made to the implementation guidance in BSI C5 BC-02 to BC-05.

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

Proof

The cloud provider can demonstrate compliance with the requirements by submitting appropriate documentation (e.g. sample contracts, contract templates or contract instances). By means of a test use of the service (in particular, insight of whether content is displayed during the registration for the service use), the cloud provider can demonstrate that it has implemented a procedure according to which the legally binding Commissioned Data Processing Agreement containing these regulations is concluded. In particular, the completeness and the sufficient level of detail to describe the TOMs must be demonstrated (e.g. specification of the TOMs in orientation on the protection goals).

No. 1.8 – Return of data media and erasure of data; demonstrating compliance and allowing for and contribute to audits (Art. 28 (3) subpara. 1 sent. 2 lit. g) and h) GDPR)

Criterion

(1) The obligations of the cloud provider to return all data media[23] (containing personal data) and return all personal data or irreversibly delete all personal data after the end of the data processing must be determined in a legally binding Commissioned Data Processing Agreement.

(2) The obligations of the cloud provider to make available all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller must be determined in a legally binding Commissioned Data Processing Agreement.

Explanation

If the cloud provider is obligated to store or keep data due to legal obligations from Union or Member State law even after the end of the Commissioned Data Processing, these data are not to be deleted. A legal obligation from third country law is not sufficient in this regard.

[22] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

[23] ISO/IEC 2382:2015, Information technology — Vocabulary, 2121321, "data medium": material in or on which data can be recorded and from which data can be retrieved.

Every cloud provider is obligated to allow the controller to demonstrate that its chosen processor complies with the obligations laid down in Art. 28 GDPR either by providing the relevant information or by allowing audits, including on-premise-inspections, of its service. This is the only way the controller can ensure that the processing is carried out in compliance with the GDPR. The obligation of the provider is an active one, i.e. it must not just “allow for" but also "contribute to”. Related audits may include general inspections, management system audits, technical tests, and certifications.

Implementation guidance

“The contract shall include details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing that are relevant to demonstrate compliance with the obligations laid down in Article 28 GDPR. For instance, the relevant portions of the processor’s records of processing activities may be shared with the controller. The processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on the functioning of the systems used, security measures, how the data retention requirements are met, data location, transfers of data, who has access to data and who are the recipients of data, sub-processors used, etc.”[24]

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

In regard to demonstrating compliance and allowing for and contribute to audits, reference is made to the implementation guidance in the EU Cloud CoC Section 5.5.3 “Approach for Customer audits”.

Proof

The cloud provider can demonstrate compliance with the requirements by submitting appropriate documentation (e.g. sample contracts, contract templates or contract instances). By means of a test use of the service (in particular, insight of whether content is displayed during the registration for the service use), the cloud provider can demonstrate that it appropriately communicates its obligations of returning data media and returning data to the cloud user and to erase data after the Commissioned Data Processing has ended.

The cloud provider can demonstrate compliance for providing the necessary information by submitting appropriate documentation verifying that the cloud provider actively undertakes means to make information available and allows for and contributes to audits carried out by the controller or other auditors mandated by it. By means of a test use the cloud provider can demonstrate that relevant information is available on demand.

[24] EDPB’s guidelines 07/2020 on the concepts of controller and processor in the GDPR, V. 2.1, § 143.

Chapter II: Rights and obligations of the cloud provider

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

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

Criterion

(1) The cloud provider must conduct a state-of-the-art risk analysis with regard to data security and it must maintain a data security program[25], which corresponds to its protection category and is appropriate for the specific risks of its data processing operations in particular, which can result from destruction, loss, alteration, unauthorised disclosure of and unauthorised access to personal data. During the risk-assessment, the cloud provider must particularly consider specific risk scenarios relevant for criteria in No. 2 and corresponding TOMs.

(2) The cloud provider must maintain a description of all categories of data for which it can offer processing with its cloud service.

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

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

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

(6) The data security program must be reviewed at regular intervals (i.e. at least annually, and after each major change) to ensure that it is up to date and appropriate and be updated if necessary. If the data security program needs to be updated, the cloud provider must inform the cloud user before the update is being effected.

(7) The data security program must describe which of the data processing operations are performed by the cloud provider itself and which of the data processing operations are performed by the involved sub-processors.

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

(9) If the data security program demands security measures from the cloud user, the cloud user must be informed of this in writing or in electronic form before the data processing starts or before changes to it are made.

Explanation

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

Implementation guidance

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

[25] A data security program documents protection principles, identified risks, and determined TOMs to safeguard processed data, among others. Often the term data security concept is used alternatively.

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 should be analysed and evaluated:

1) Evaluation of the impact on the organisation, technology and service provision due to a security failure and consideration of the consequences of a loss of confidentiality, integrity, or availability;
2) Evaluation of the realistic probability of such a security failure, taking all conceivable threats and security gaps into account;
3) Assessment of the possible level of damage to the data subject's fundamental rights and freedoms;
4) Verification that all possible risk management options have been identified and evaluated;
5) Assessment of whether the residual risk is acceptable or if a countermeasure is required.

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

Reference is made to the implementation guidance in BSI C5 OIS-02, OIS-03, OIS-05, OIS-06, OIS-07, OPS-010, SP-01, SP-02, SP-03, OPS-18, SIM-01, and HR-04.

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

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

Reference is made to the implementation guidance in the SDM module 11 "Storage", module 41 "Plan and specify", module 42 "Documentation", and module 51 "Control access to data, systems and processes".

Reference is made to the implementation guidance in the SDM, Section D3.

Proof

The cloud provider submits the data security program and all other documents, if applicable, which contain detailed information about the risk assessment procedure. These documents list all identified risks with details of the respective probability of their occurrence and their severity. The documents also contain the considerations that the cloud provider has made when choosing the data security measures and describe the data security measures for addressing the risks (e.g. documentation of planned measures in the company's internal ticket system and reference to the risks addressed by these measures). In particular, the cloud provider can also submit documents regarding the processes in the event that a risk materialises (e.g. in the form of company guidelines). In addition, documentation should be provided on the separation of the areas of responsibility between the cloud provider and sub-processors and between the cloud provider and cloud user.

Insofar as the data security program requires security measures to be taken by the cloud user, the cloud provider can submit for example, existing protocols, contracts, process specifications for notification to the cloud user. If the cloud user is informed electronically, for example during the online registration process for the cloud service, the cloud provider can also demonstrate the compliant notification information being given to the cloud user by means of a test use of the service.

The cloud provider must ensure that the submitted documents verify that the data security program is up-to-date and continuously developed further (e.g. by time stamps, versioning history or logs of further development).

The cloud provider may enable an employee interview as support in order to demonstrate the completeness and implementation of the above points in the company.

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

Criterion

Protection category 1

(1) The cloud provider must ensure by means of risk-appropriate TOMs that its premises and facilities are protected against damage caused by force majeure[26] and that unauthorised persons have no entry to the premises and data processing facilities so as to prevent unauthorised physical access to personal data and the possibility of manipulation of the data processing facilities.

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

(3) The measures must be appropriate to regularly prevent unauthorised persons from obtaining entry due to technical or organisational errors, including operating errors of the cloud provider, or negligent acts of third parties. At least, the cloud provider must implement and document a set of security requirements for each security zone.

(4) The cloud provider must review periodically (i.e. at least annually or in case of major change) and, if necessary, update the current status and adequacy of the authorisations that are required for the entry to rooms and facilities.

(5) Every authorised entry must be logged.

Protection category 2 and 3

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

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

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

Explanation

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

Implementation guidance

Protection category 1

To ensure that unauthorised persons do not get entry to premises and data processing facilities, entry to the computing centre should be continuously monitored by video surveillance systems, motion sensors, alarm systems, and trained security staff. Entry to areas where personal data are processed should be secured with a suitable two-factor authentication procedure, e.g. consisting of an entry card and a secret PIN (s. ISO/IEC 27002 no 11.1.2). Entry rights should be reviewed and updated regularly (at least annually, and after each major change)) and withdrawn, if necessary. Access to premises and processing facilities should be documented in a physical log or an electronic audit trail, which are to be stored securely and be monitored (s. ISO/IEC 27002 no. 11.1.2). The signing in and signing out of visitors should be noted with the date and the time.

Facilities should be protected against fire, water, earthquakes, explosions, disturbances and other forms of natural hazards and human-made hazards by structural, technical and organisational measures (s. BSI C5 PS-05). These include, among other things, early fire detection and extinguishing systems, the implementation of regular fire drills and fire safety inspections to check compliance with fire protection measures, the embedding

[26] Force majeure must be understood as referring to abnormal and unforeseeable circumstances which were outside the control of the party by whom it is pleaded and the consequences of which could not have been avoided in spite of the exercise of all due care. Since the concept of *force majeure* does not have the same scope in the various spheres of application of EU law, its meaning must be determined by reference to the legal context in which it is to operate. C-640/15, ECLI:EU:C:2017:39.

of sensors to monitor temperature and humidity and the equipping of all buildings with lightning protection devices. Expert advice can be obtained to prevent possible damage (s. ISO/IEC 27002 no. 11.1.4).

Protection category 2 and 3

The implementation guidance for protection category 1 apply.

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

Physical entry controls should be developed and used in particular against malicious attacks or accidents, and at the same time adapted to the technical and economic conditions of the cloud provider, which are set out in the data security program. The building structure of the location should be physically solid, and all external doors should be adequately protected against unauthorised entry with the help of control mechanisms (e.g. barriers, alarm devices, locks) (s. ISO/IEC 27002 no. 11.1.1). Burglar-resistant material (e.g. according to DIN EN 1627 resistance class RC 2) and corresponding locking devices should be installed on the outer doors and windows (s. BSI C5 PS-03). All outer doors and all accessible windows should be monitored by burglar alarm systems.

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

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

Reference is made to the implementation guidance in BSI C5 OIS-04, PS-01, PS-03, PS-04, PS-06, PS-07.

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

Proof

As proof of compliance with the requirements, the cloud provider submits the relevant documentation relating to entry control and the protection against damages due to natural phenomena. This includes the documentation of the TOMs in the data security program, authorisation concepts, and process instructions/concepts/guidelines, e.g. site security guards, video surveillance, visitor regulations, intrusion detection systems, locking systems and authorisations.

The implementation, appropriateness, and (continuous) operation of entry controls must be demonstrated in the course of on-site assessments. The cloud provider must demonstrate the availability and reliability of defined entry controls and the employees' familiarity with the relevant instructions. In addition, it must prove the actual implementation of the measures on site in accordance with the documentation (e.g. site security service active, video surveillance available, records and logs are available).

The cloud provider should also allow employee interviews in order to demonstrate that training and awareness-raising measures (e.g. for social engineering prevention) are carried out and that employees are aware of the relevant rules of conduct (e.g. dealing with external persons). The maintenance and current status of the documentation of measures should be demonstrated by appropriate documentation (e.g. time/date stamp of key registries).

For protection categories 2 and 3, a cloud provider should submit the process documentation for logging unauthorised entry and attempted entries in order to demonstrate whether continuous logging is carried out. The actual logging can be verified by submitting entry and event logs or by means of electronic audit trails. As part of an on-site assessment, it can be demonstrated that unauthorised entry and entry attempts are afterwards. For protection category 3, these verifications apply analogously to the detection of whether every authorised entry has been logged.

No. 2.3 – Admission control[27]
(Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

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

(2) The cloud provider must periodically review (i.e. at least annually or in case of major change) the current status and adequacy of rights that are required for admission to data processing systems and update them if necessary.

(3) The cloud provider must verify the admission of authorised persons via the internet by means of a two-factor authentication procedure. Admission via the internet must be implemented through the use of state-of-the-art transport encryption.

The measures for admission control must be designed to regularly prevent unauthorised persons from being admitted to data processing systems due to technical or organisational errors, including operating errors of the cloud provider, or due to negligent acts of the cloud user or third parties. The measures must ensure that, by documenting and implementing procedures to grant, update and remove access rights, an unauthorised admission to data processing systems is prevented.

Protection category 2

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

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

Protection category 3

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

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

Explanation

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

Implementation guidance

Protection category 1

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

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

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

[27] Admission refers to every form of approach to data processing systems. In contrast, access refers to every form of actual use of data processing systems.

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

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

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

Protection category 2

The implementation guidance for protection category 1 apply.

Admission should be adequately monitored and protected to detect attacks. Among other things, virus protection and repair programs should be used, which enable signature and behaviour-based detection and removal of malicious programs (see BSI C5 OPS-04, OPS-05).

Secret authentication details (e.g. passwords, certificates, security tokens) should be provided to employees of the cloud provider or the cloud user in a proper organised procedure, provided this is subject to the cloud provider's organisational or technical procedures, whereby the confidentiality of the information will be ensured (s. BSI C5 IDM-08 and IDM-09). If the authentication details are initially assigned, it should only be valid temporarily, but no longer than 14 days. Users should also be forced to change these on first use. Interactive systems for managing passwords should be used, as well as strong passwords according to the state of the art (s. ISO/IEC 27002 no. 9.4.3).

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

Admission authorisation for cross-network access should be based on a security assessment on the basis of the customer requirements (s. BSI C5 COS-04). Administrative authorisations should be checked at least every six months (s. BSI C5 IDM-05).

Reference is made to the implementation guidance in BSI C5 OIS-04, OPS-04, OPS-05, OPS-18 to OPS-23, IDM-01 to IDM-09, COS-04, COS-05 and SIM-01 to SIM-05.

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

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

Admission should be adequately monitored and protected in order to detect attacks. To this end, among other things, vulnerabilities scanners and intrusion detection, and prevention systems should be used and annual penetration tests should be carried out to identify and remedy weak points. System components that are used for the provision of the cloud service should be hardened according to the generally accepted industry standards (s. BSI C5 OPS-23).

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

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

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

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

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

Proof

The cloud provider submits verification of admission control in the form of documentation including, for example, documentation of the TOMs in the data security program, authorisation concepts, process instructions, guidelines/concepts for passwords, documentation for authentication and encryption concepts for access (of authorised employees) and admission authorisations. The documentation must show that the admission concept and the authorisations are up-to-date and continuously updated (e.g. by means of time stamps, versioning history or update logs).

The implementation, appropriateness, and (continuous) operation of admission controls are verified in an on-site audit. It should be demonstrated by an employee interview during the audit, whether they have knowledge of the corresponding rules of conduct (e.g. the prohibition of passing on passwords) and whether measures are also carried out in accordance with the documentation (e.g. checking of the withdrawal of admission rights after employees leave the organisation). As part of a test, admission interfaces can also be checked for security (e.g. blocking employees' computers).

For protection categories 2 and 3, the cloud provider submits the process documentation to detecting unauthorised admission as evidence. The actual detection can normally be demonstrated by submitting admission and event logs or by electronic audit trails, provided that unauthorised admission has taken place. As part of the on-site audit and an interview or a test, the cloud provider can demonstrate that unauthorised admission can usually be detected afterwards. For protection category 3, the cloud provider also proves that any unauthorised admission and corresponding attempts can be subsequently detected.

No. 2.4 – Access control[28]
(Art. 32 (1) lit. b) and (2) in conjunction with Art. 5 (1) lit. f) GDPR)

Criterion

Protection category 1

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

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

(3) The cloud provider must periodically review (i.e. at least annually or in case of major change) the current status and appropriateness of the rights that are required for access to personal data and update them if necessary.

(4) The cloud provider must control (i.e. monitor and asses) and log any access to personal data.

(5) The measures must be appropriate to regularly prevent unauthorised persons from accessing personal data due to technical or organisational errors, including operating errors of the cloud provider, or due to negligent acts of the cloud user or third parties. The measures must ensure that intentional manipulation is regularly prevented.

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

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

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

Protection category 2

[28] Access refers to every form of actual use of data processing systems. In contrast, admission refers to every form of approach to data processing systems.

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

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

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

Protection category 3

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

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

Explanation

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

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

Implementation guidance

Protection category 1

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

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

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

The assignment and change of access rights for users with administrative or extensive authorisations under the responsibility of the cloud provider should take place in accordance with documented access guidelines (s. BSI C5 IDM-01, IDM-06, and PSS-08). The assignment should be personalised and to the extent necessary for the performance of the task ("need-to-know principle"). Organisational and/or technical measures should ensure that the assignment of these authorisations does not result in undesired, critical combinations that violate the principle of functional separation (e.g. assignment of authorisations for the administration of the database and the operating system). If this is not possible in selected cases, appropriate, compensatory controls should be set up to identify any misuse of these rights (e.g. logging and monitoring by a SIEM solution).

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

Reference is made to the implementation guidance in the SDM module 43 "Logging" and module 51 "Control access to data, systems and processes**".**

Protection category 2

The implementation guidance for protection category 1 applies.

Security parameters on the network, operating system (host and guest), database and application level (where relevant for the cloud service) should be appropriately configured to prevent unauthorised access (s. BSI C5 IDM-01, IDM-06, PSS-05, PSS-06, PSS-07, and PSS-09). The cloud service should be continuously monitored for attacks and security incidents to be able to identify suspicious activities (e.g. extraction of large amounts of data from several clients), attacks and security incidents on time and initiate appropriate and timely reactions.

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

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

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

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

Guidelines and instructions with TOMs for the proper use of mobile devices in the cloud provider's area of responsibility, which allow access to IT systems for the development and operation of the cloud service, should be documented, communicated and provided (s. also BSI C5 OPS-04).

Reference is made to the implementation guidance in BSI C5 OIS-04, OPS-04, OPS-05, OPS-10, OPS-18 to OPS-23, IDM-01 to IDM-09 and COS-01, KOS-04, KOS-05, and SIM-01 to SIM05.

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

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

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

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

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

Proof

To demonstrate compliance with the requirements, the cloud provider presents the documentation for access control including documentation of the TOMs under the data security program, authorisation concepts, process instructions, regulations for privileged access, access guidelines and logs of administrative access and activities. The submitted documents must show that the access concept and the authorisations are up-to-date and continuously updated (e.g. by means of time stamps, versioning history or update logs).

If employees of the cloud provider have privileged access to personal data on the instructions of the cloud user, a cloud provider will submit a representative sample of legally binding Commissioned Data Processing Agreement s

with the cloud user or other documents with instructions given by the cloud user to demonstrate that the instructions are documented and regulated.

The implementation and appropriateness of TOMs for access control are verified by (security) tests and an on-site audit. The cloud provider enables security tests to be carried out (e.g. checking for encryption, securing administrative activities, firewall configuration, etc.) to prove the security and appropriateness of the technical access security measures. Administrative activities can also be carried out on a test basis and their logging can be verified.

The cloud provider should prove by employee interviews during the audit that they are aware of the relevant rules of conduct (e.g. prohibition of passing on passwords) and that measures are also carried out in accordance with the documentation (e.g. checking the withdrawal of access rights after employees leave the organisation).

For protection categories 2 and 3, a cloud provider submits the process documentation for detecting unauthorised access. The actual detection can usually be demonstrated by submitting access and event logs or by electronic audit trails in the case that unauthorised access has taken place. As part of the on-site audit and an interview or test, it can be proven whether unauthorised access can usually be detected afterwards. For protection category 3, a cloud provider also proves that any unauthorised access and corresponding attempts can be detected afterwards.

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

Criterion

Protection category 1

(1) The cloud provider must use state-of-the-art transport encryption for data transmission processes or configure interfaces in such a manner that this is a requirement. It must also document the official standards or the state-of-the-art specifications used to define its TOMs regarding transport encryption. The transport encryption used must ensure that personal data cannot be read without authorisation during electronic transmission.

(2) The measures must be appropriate to regularly prevent attacks by unauthorised persons based on technical or organisational errors, including operating errors of the cloud provider or its employees, or negligent acts of the cloud user or third parties. Moreover, the measures must be suitable to prevent any negligent disclosure of data to unauthorised persons by the cloud provider and its employees. Protection must prevent intentional interference. Whenever the transmission is encrypted, the encryption keys must be securely stored in regard to official standards or the state-of-the-art and access to the key must be controlled (no. 2.4).

(3) The cloud provider must automatically log the metadata[29] of all data transmission operations, including those of recipients and those sent from and to the cloud user or sub-processor. No. 2.6 (1) applies accordingly.

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

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

Protection category 2

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

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

Protection category 3

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

[29] Metadata refers to information that describes other data. It provides context, attributes and details about a particular set of data, helping to organize, understand, and manage it. In simpler terms, metadata is data about data.

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

Explanation

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

Implementation guidance

Protection category 1

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

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

Reference is made to the implementation guidance in BSI C5 CRY-01, CRY-02, COS-01, COS-02, COS-06 and COS-08.

Reference is made to the implementation guidance in the SDM module 43 “Logging”.

Protection category 2

The implementation guidance for protection category 1 apply.

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

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

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

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

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

Proof

The cloud provider submits the documentation of the transmission of data and transport encryption as proof of the compliance with the requirements, including the TOMs in the data security program, process instructions, guidelines, protocol and log data, result logs of internal/external audits, list of the security scanners in use, documentation of infrastructure access via APIs, documents for key management (in particular, access and storage of keys), documents relating to the transport of data media and documentation of the data transmission processes.

The cloud provider must prove by means of (security) tests that the documentation corresponds to the actual implementation of the measures and that the measures are effective and up to date. An employee interview, e.g. regarding the knowledge of the relevant guidelines and instructions, and a sample test of the reaction by relevant employees to the implementation of specified guidelines and instructions can be used as proof.

For protection categories 2 and 3, a cloud provider submits the documentation for the detection of unauthorised reading, copying, changing or removing of personal data. The actual detection can be demonstrated in the normal case by checking event logs, logs of defence against and detection of attacks or electronic audit trails, if unauthorised activities have taken place. For protection category 3, a cloud provider proves analogously whether any unauthorised reading, copying, modification or removal of data and corresponding attempts can be detected afterwards.

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

Criterion

Protection category 1

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

(2) The cloud provider must design the logs in such a way that entries, alterations, and erasures can generally be traced, even in the event of technical or organisational errors, including operating errors of the cloud provider or its employees, or in case of negligent acts of the cloud user or third parties. The cloud provider must provide measures ensuring that intentional manipulation is regularly prevented by at least storing all log data in an integrity-protected form that allow its evaluation

(3) The cloud provider must establish procedures for analysing and auditing logs to effectively identify anomalies and incidents, and subsequently raise alerts. It is to take those events into consideration when reviewing the risk analysis (No. 2.1 [6]).

Protection category 2

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

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

Protection category 3

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

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

Explanation

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

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

Implementation guidance

Protection category 1

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

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

The generated logs should be kept on central logging servers, where they are protected against unauthorised access and changes (s. BSI C5 OPS-14). Log data should be erased without undue delay if they are no longer required for the fulfilment of the purpose.

Reference is made to the implementation guidance in the SDM module 43 “Logging”.

Protection category 2

The implementation guidance for protection category 1 apply.

Authentication should take place between the central logging servers and the logged (virtual) servers to protect the integrity and authenticity of the transmitted and stored information (s. BSI C5 OPS-14). The transmission should be carried out using state-of-the-art encryption or via a separate administration network (out-of-band management).

Access and management of the logging and monitoring functionalities should be limited to selected and authorised employees of the cloud provider. Changes to the logging and monitoring should be reviewed and approved in advance by independent and authorised employees (s. BSI C5 OPS-16).

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

Reference is made to the implementation guidance in BSI C5 OPS-10, OPS-11, OPS-12.

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

Protection category 3

The implementation guidance for protection category 1 and 2 apply.

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

The availability of the logging and monitoring software should be monitored independently (s. BSI C5 OPS-17). If the logging and monitoring software fails, the responsible employees should be informed immediately. The logging and monitoring software should be redundant so that logging and monitoring can also be carried out in the event of failures.

The generated logs allow a definitive identification of user access at the tenant level so as to support (forensic) analyses in the event of a security incident (see BSI C5 OPS-15).

Reference is made to the implementation guidance in BSI C5 OPS-14 to OPS-17.

Proof

The cloud provider can demonstrate compliance with the requirements by documenting in the data security program how it ensures compliance with data protection principles by defining the subject and scope of the logging, storage, the integrity protection and erasure of logs, and the use of log data. Other documents such as rights authorisation (in particular user and administrator authorisations), process instructions, guidelines, protocol and log data, results logs of internal/external audits and risk analyses can serve as proof.

The implementation and appropriateness of this logging concept should be verified by representative samples during ongoing operations (e.g. proof that log entries are generated when personal data are entered, changed and erased). Security tests can also be used to verify the applied measures for the protection of logs against manipulation.

For protection categories 2 and 3, a cloud provider submits the documentation of the detection of log manipulations. The actual detection can regularly be demonstrated by submitting event logs, protocols for the defence against and detection of manipulations or by means of electronic audit trails, provided that manipulations have taken place. For protection category 3, a cloud provider proves analogously whether every manipulation and, if possible, every corresponding attempt can be detected afterwards.

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

Criterion

Protection category 1

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

(2) If the type of the Commissioned Data Processing with the cloud user requires the de-pseudonymisation of the data, the cloud provider must ensure that the data are de-pseudonymised only on the cloud user's documented instructions.

Protection category 2 and 3

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

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

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

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

(7) The cloud provider must guarantee that it continuously (at least annually) monitors technical developments in the field of pseudonymisation procedures and that its procedures comply with the state of the art (as exemplified in the implementation guidance).[30]

Explanation

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

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

Implementation guidance

Protection category 1

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

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

Protection category 2 and 3

The implementation guidance for protection category 1 apply.

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

[30] The state of the art embodies what is currently and generally accepted as best practices, technologies, methodologies, and strategies used to protect information systems. The state of the art does not necessarily imply the most technologically advanced solution but comprises robust technologies and processes, and skilled personnel to defend against evolving data protection threats effectively.

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

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

Proof

For protection category 1, the cloud provider submits documentation on the data processing process, particularly regarding pseudonymised data. A test use of the service with pseudonymised data can serve as proof that processing is performed while maintaining pseudonymity. If the type of processing order with the cloud user requires de-pseudonymisation of the data, a cloud provider submits the legally binding Commissioned Data Processing Agreement with the cloud user or other documents that are used for instructions being issued by the cloud user.

For protection categories 2 and 3, a cloud provider submits documentation that demonstrates the ways in which pseudonymisation is implemented, identifying data are stored securely and protected against manipulation, and pseudonymised data are processed (e.g. submission of TOMs documentation, process instructions, guidelines, protocol and log data, result logs of internal/external audits and the risk analysis).

The implementation, appropriateness, and effectiveness of the pseudonymisation procedures and the measures to protect the additional information for identification are determined for protection categories 2 and 3 by means of representative samples in the context of a (security) test. The cloud provider can also demonstrate the type of programs it uses, the programming for pseudonymisation and their configuration, in the context of an asset test and allow a random review of pseudonymised data records. An employee interview as part of an audit can also serve as evidence by comparing the measures specified in the documentation with the measures actually implemented for protection categories 2 and 3 (e.g. compliance with guidelines and protective measures, awareness of the instructions for de-pseudonymisation).

In addition, the cloud provider submits documentation (e.g. logs, versioning history) that demonstrates that it continuously follows the technical development in the field of pseudonymisation procedures. This can also be proven in the context of an asset test (e.g. proof of changes to the program code for pseudonymisation, updating of libraries, etc.). An employee interview can also demonstrate that they know and implement the current recommendations for pseudonymisation.

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

Criterion

Protection category 1

(1) The cloud provider ensures by TOMs[31] being put in place that anonymization[32] cannot be revoked (i.e. re-identifying personal data in an anonymized data set).

Protection category 2 and 3

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

(3) If the anonymisation is carried out by the cloud provider, the cloud provider must ensure that it continuously follows the technical developments in the field of anonymisation processes, and that its processes comply with the state of the art.[33]

[31] Technical safeguards may comprise the prevention of automatic data aggregation, synthesizes etc. which could lead to the revocation of anonymization, as well as managing access rights of its authorised employees to prevent malicious behavior. Organizational protection measures ensure, among others, that employees do not engage in behavior aiming to revoking anonymization, such as asking cloud users about their anonymization practices to exploit potential vulnerabilities or weak points of applied anonymization techniques.
[32] TOMs regarding anonymization therefore must comply with official standards or the state-of-the-art.
[33] The state of the art embodies what is currently and generally accepted as best practices, technologies, methodologies, and strategies used to protect information systems. The state of the art does not necessarily imply the most technologically advanced solution but comprises robust technologies and processes, and skilled personnel to defend against evolving data protection threats effectively.

Explanation

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

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

Implementation guidance

Protection category 1

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

Protection category 2 and 3

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

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

Proof

For protection category 1, the cloud provider submits documentation on the data processing process, particularly regarding anonymous data. As part of a test use of the service with anonymous data, it can be demonstrated that processing is performed while maintaining anonymity.

For protection categories 2 and 3, the cloud provider submits documentation that explains the ways in which the cloud provider implements anonymisation and processes anonymised data, and which anonymisation procedures are used or offered (e.g. documentation of TOMs, process instructions, guidelines, protocol and log data, result logs of internal/external audits and risk analysis).

The implementation and appropriateness of the anonymisation procedure is determined for protection categories 2 and 3 in the context of an inspection and/or test using representative samples. For this purpose, the type of programs that are used, the anonymisation programming and its configuration should be checked as part of an asset test. In addition, a random check of data records should be carried out. An employee interview can also serve as evidence by comparing the measures specified in the documentation with the measures actually implemented for protection categories 2 and 3 (e.g. interviews regarding guidelines and regulations for anonymisation).

By submitting documentation (e.g. logs, versioning history), a cloud provider proves for protection categories 2 and 3 that that it continuously follows technical developments in the area of anonymisation. This can also be demonstrated in the context of an asset test (e.g. proof of changes to the program code for anonymisation, updating of libraries, etc.).

No. 2.9 – Encrypting stored data[34]
(Art. 32 (1) lit. a) GDPR)

Criterion

Protection category 1

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

(2) If the cloud provider offers data encryption procedures, it must fulfil criteria for protection category 2.

Protection category 2

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

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

[34] Note that stored data also covers backups of stored data.

(5) The cloud provider must continuously monitor technical developments in encryption. The measures of the cloud provider, particularly secure key management, must comply with the state of the art (as exemplified in the implementation guidance).[35]

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

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

Protection category 3

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

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

(10) The cloud provider must ensure that its assistance measures in the form of documentation and support for implementing encryption comply with the state of the art (as exemplified in the implementation guidance).[36]

Explanation

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

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

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

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

Implementation guidance

Protection category 1

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

Protection category 2

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

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

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

Reference is made to the Technical Guidelines BSI TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths" in the respective current version.

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

[35] The state of the art embodies what is currently and generally accepted as best practices, technologies, methodologies, and strategies used to protect information systems. The state of the art does not necessarily imply the most technologically advanced solution but comprises robust technologies and processes, and skilled personnel to defend against evolving data protection threats effectively.

[36] The state of the art embodies what is currently and generally accepted as best practices, technologies, methodologies, and strategies used to protect information systems. The state of the art does not necessarily imply the most technologically advanced solution but comprises robust technologies and processes, and skilled personnel to defend against evolving data protection threats effectively.

Protection category 3

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

Proof

For protection category 1, the cloud provider submits documentation on the data processing process, particularly with regard to the storage of encrypted data. Successful storage can be proven as part of a test use of the service with encrypted data.

For protection categories 2 and 3, a cloud provider submits documentation to demonstrate that the encryption procedures offered and used meet the current technical requirements (e.g. documentation of the TOMs, process instructions, guidelines, protocol and log data, result logs of internal/external audits, risk analysis). The implementation and appropriateness of the encryption procedures is determined for protection categories 2 and 3 by means of an inspection and/or test using representative samples. For this purpose, the type of programs that are used, the programming for encryption and its configuration among other things should be verified as part of an asset test. In addition, a random review of datasets should be conducted. By submitting documents (e.g. logs, versioning history), the cloud provider proves for protection categories 2 and 3 that that it continuously follows the technical development in the field of encryption, checking the appropriateness of the procedure and updating the procedure and the documentation if necessary (e.g. proof of changes to the program code for encryption, updating of libraries, etc.). An employee interview can also demonstrate that the employees know and implement the current recommendations for encryption. The cloud provider should submit protocols that prove that it has checked the encryption techniques by suitable technical tests.

The cloud provider submits access and event logs of the access to keys for protection category 3. In addition, it can submit other documents such as the user documentation for encryption/decryption, documentation of encryption procedures or protocols from a qualified IT security committee (which can be verified by training), wherein the technical procedures for encryption/decryption are also regularly reflected.

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

Criterion

Protection category 1

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

(2) The cloud provider must prevent violations of the separation principle caused by technical or organisational errors, including operating errors of the cloud provider or its employees or negligent acts of the cloud user or third parties.

Protection category 2

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

(4) The cloud provider must offer protection against known attack scenarios threatening the separation principle. The cloud provider is regularly able to detect intentional violations of the separation principle (afterwards).

Protection category 3

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

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

Explanation

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

Regarding the separation of the data processing according to the different purposes of the processing, it must be noted that the cloud provider merely has to offer the technical opportunity for separate processing, while the

implementation of separate data processing in accordance with processing purposes is the responsibility of the cloud user.

Implementation guidance

Protection category 1

Data should be separated securely and strictly on jointly used virtual and physical resources (storage network, main memory) according to a documented concept (s. BSI C5 OPS-24). A technical separation of the stored and processed data of the cloud users in jointly used resources can be achieved by means of firewalls, access lists, tagging (labelling of the data stock), VLANs, virtualisation and measures in the storage network (e.g. LUN masking).

Reference is made to the implementation guidance in BSI C5 OPS-24 and COS-06.

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

Reference is made to the implementation guidance in the SDM module 50 “Separation”.

Protection category 2

The implementation guidance for protection category 1 apply.

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

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

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

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

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

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

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

In case of IaaS/PaaS, the secure separation is ensured by means of physically separated networks or strongly encrypted VLANs (s. BSI C5 COS-06).

Protection category 3

The implementation guidance for protection categories 1 and 2 apply.

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

Proof

The cloud provider can demonstrate compliance with the requirements by documenting in the data security program 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 processing purposes. In addition, it can submit, for example, the documentation of the TOMs, process instructions, guidelines, and result logs of internal/external audits, risk analyses, and product descriptions as evidence.

The actual implementation of the measures (e.g. separate databases) should be verified by testing the separation (e.g. the programs used or the program code, checking for separate databases) and by means of security tests (e.g. penetration tests to detect the security level of the client separation). An interview of relevant employees as part of an audit (e.g. for knowledge of guidelines, etc.) can be provided as evidence.

For protection categories 2 and 3, a cloud provider presents documentation to prove the detection of intentional violations of the separation principle. The actual detection can normally be proven by submitting event logs, logs for defence against and detection of attacks or by means of electronic audit trails.

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

Criterion

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

Restorability class 1

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

Restorability class 2

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

Restorability class 3

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

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

Explanation

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

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

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

Incidents are deemed force majeure, infrastructure disruptions and malfunctions, operating errors and intentional interference.

Implementation guidance

Restorability class 1

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

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

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

Reference is made to the implementation guidance in BSI C5 OPS-01 to OPS-03, OPS-06 to OPS-10.

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

Reference is made to the implementation guidance in the SDM module 11 “Storage”.

Restorability class 2

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

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

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

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

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

Restorability class 3

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

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

Proof

The cloud provider can demonstrate compliance with the requirements by documenting in the data security program the events it has considered, which could lead to a physical, organisational or technical incident, and which concrete measures it has taken to restore the data after an incident.

Further documents as proof of restorability can be in particular the documentation of the TOMs, process instructions, guidelines, protocols for test runs of data restoring, results of internal/external audits, risk analyses and product descriptions.

The implementation and appropriateness of the appropriate TOMs should be verified by representative samples as part of an audit. The implementation can also be demonstrated by interviews of the relevant employees (e.g. for knowledge about guidelines and process instructions for restoration, etc.). The testing or inspection of server rooms and the assessment of measures taken and the applied techniques (e.g. redundant servers) for restorability can be submitted as evidence. A failure and restoration can be simulated on a test basis and employees can be observed in the process to demonstrate compliance with the process documentation.

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

Criterion

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

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

(3) The cloud provider processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the

processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(4) Within the framework of standardised bulk transactions, the cloud provider must guarantee the compliance with a concrete and comprehensible service description for the services it is technically able to perform, in order to enable the cloud user hereby to instruct the cloud provider via his/her specific choice of services for Commissioned Data Processing. In addition, it must enable the cloud user to issue instructions by means of software orders (or other means) that are (automatically) performed and documented.

Implementation guidance

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

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

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

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

Reference is made to the implementation guidance in BSI C5 OIS-04, OPS-04, OPS-05, OPS-18 to OPS-23, and COS-01, COS-04, COS-05, and SIM-01 to SIM-05 for the protection of the cloud service from internal and external attacks and manipulations.

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

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

Proof

As evidence, the cloud provider submits verification of the compliance with instructions in the form of documentation including, for example, documentation of the TOMs, process instructions (especially for administrators), guidelines, logging of instructions and documented measures for protection and manipulation prevention.

In the case of individual legally binding Commissioned Data Processing Agreement s with cloud users, the cloud provider submits a sample of the legally binding Commissioned Data Processing Agreement s to be able to demonstrate the implementation of and compliance with the documented instructions with the actual conduct of the employees and the cloud service. For this purpose, a test instruction can be simulated up as a function in the cloud service or relevant employees can be instructed to perform an instruction as part of an audit.

In the case of bulk transactions, the cloud provider submits a service description for the technically feasible services and instructions by software commands so that these can be compared with the actually possible interaction in the cloud service (e.g. in the context of a test service use). The cloud provider should submit logs of the continuous documentation of issued instructions and/or software commands from cloud users (e.g. log entries, time stamps, versioning of log files) as evidence. As part of an audit, an interview or observation of relevant employees (e.g. as to their knowledge of instructions from cloud users and guidelines for following them, etc.) can be conducted for verification.

As proof of the compliance with the requirements, the cloud provider submits notifications to the cloud user of legal requirements for processing, which are not covered by instructions, in fulfilment of legal obligations under Union or Member State law, where such legal requirements apply. Verification can also be provided in the form of documentation including, for example, documentation of the TOMs or process instructions, e.g. how to handle inquiries from law-enforcement authorities concerning the surrender of data or the manner in which the cloud user is to be informed about these legal requirements.

No. 4 – Reporting duty of the cloud provider

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

Criterion

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

Explanation

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

Implementation guidance

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

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

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

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

Proof

The cloud provider can demonstrate compliance with the requirements by documenting the ways in which it reviews instructions, recognises doubts about their legitimacy under data protection law, and how it notifies the cloud user of this before executing the instruction. This can include the documentation of the TOMs, process instructions, guidelines, logging of instructions, documentation of the relevant mechanisms and reporting channels, and documented processes for reviewing instructions. If a deviation is suspected, a cloud provider can also submit documented communication to cloud users that has taken place.

An interview of relevant employees (e.g. regarding knowledge of guidelines and procedural steps in case of doubts, etc.) can be conducted as part of an audit for further verification. In addition, by means of employee observation in the course of which an illegal instruction is given as a test, it can be demonstrated that the processes for including and processing the instruction are performed.

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

Criterion

The cloud provider must notify the cloud user always without undue delay and as a rule in advance whenever the location of data processing will change from the one that is specified in the legally binding Commissioned Data Processing Agreement (No. 1.5) during the period of validity of the legally binding Commissioned Data Processing Agreement.

Implementation guidance

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

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

Proof

The cloud provider can demonstrate compliance with the requirements by submitting documents on measures and responsibilities it has implemented to inform the cloud user about changes of the data processing location (e.g. documentation of the TOMs, process instructions, guidelines, documented process for communication to the cloud user, documentation of the relevant mechanisms and reporting channels). A cloud provider can also submit information that has already been provided to cloud users about changes to data processing location.

By executing the processes on a test basis as part of an audit (e.g. simulation of a planned change of location), it can be demonstrated that all information necessary regarding the change of location is communicated to the cloud user in an appropriate manner. An interview of relevant employees (e.g. about knowledge of guidelines, etc.) can be conducted for further verification.

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

Criterion

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

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

Explanation

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

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

Implementation guidance

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

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

Reference is made to the implementation guidance in BSI C5 HR-05 and HR-06.

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

Proof

A cloud provider submits a template document of the declaration of commitment and the process documentation for the confidentiality obligation and adapting declarations of commitment (e.g. if the tasks and processing authorisations of employees change).

Compliance with these requirements can be demonstrated in all process constellations in the course of an audit by interviews of employees (e.g. survey of whether employees have been subjected a confidentiality obligation and if they are aware of the confidentiality obligations involved). An employee observation can also be conducted by testing a change of processing rights so as to simulate the adjustments of declarations of commitment.

No. 6 – Support for the cloud user when safeguarding the rights of the data subjects[37]

Explanation

As the controller, the cloud user is responsible for ensuring that the rights of data subjects are fulfilled. Insofar as it is not possible for it to do so, the cloud provider as the processor must provide support to it. In this case, the cloud

[37] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

provider must provide a point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of the data subject without undue delay.

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

No. 6.1 – Provision of information[38]
(Art. 13 or 14 in conjunction with Art. 12 (1) and Art. 5 (1) lit. a) GDPR)

Criterion

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

(2) The cloud provider must document instructions received from the cloud user for fulfilling the cloud user´s obligation to inform or when assisting in it.

Explanation

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

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

Implementation guidance

As far as personal data are concerned that only the cloud provider can grant access to (e.g. server logs),, an organisational point of contact for the cloud user with appropriate availability and authorisations, who can initiate the fulfilment of the rights of the data subject without undue delay should be provided. The cloud user's instructions can be documented by means of a ticket system.

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

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

Proof

The cloud provider can demonstrate compliance with the requirements by submitting documents on measures that it has taken to enable the cloud user to provide information to a data subject or arrange for this to be done by the cloud provider (e.g. by mechanisms and reporting channels, service descriptions). Process documentation and logs can also be used to verify that the information has in fact been provided.

In the course of an inspection, the cloud provider can provide information as a test to demonstrate that this provision of information is possible (e.g. by means of a technical function within the cloud service or by manual inquiries with the cloud service support).

The cloud provider should submit logs of the ongoing documentation of instructions and/or software commands issued by cloud users as evidence of the fulfilment of the provision of information (e.g. log entries, time stamps, versioning of log files). As part of an audit, interviews or observation of relevant employees (e.g. to be aware of instructions from cloud users and guidelines for following them, etc.) can also be conducted for verification.

[38] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

No. 6.2 – Right of access[39]
(Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 15 GDPR)

Criterion

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

(2) The cloud provider must document instructions received from the cloud user on the fulfilment of the cloud user´s obligation of the granting of right of access or when assisting in it.

Explanation

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

Implementation guidance

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

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

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

Proof

The cloud provider can demonstrate compliance with the requirements by submitting documents on the measures it has taken to enable the cloud user to provide information to a data subject or arrange for this to be done by the cloud provider (e.g. by mechanisms and reporting channels, service descriptions). Process documentation and logs can also be used to verify that the information is in fact provided.

As part of an inspection, a representative sample disclosure can be carried out to check whether disclosure and provision of the data are possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support). The cloud provider should submit logs of the continuous documentation of instructions and/or software commands issued by cloud users as evidence of the fulfilment of the provision of information (e.g. log entries, time stamps, versioning of log files).

No. 6.3 – Rectification and completion[40]
(Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 16 GDPR)

Criterion

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

(2) The cloud provider must document instructions received from the cloud user for the fulfilment of the cloud user´s obligation for granting the right to rectification and completion or when assisting in it.

Explanation

In accordance with Art. 16 GDPR, the cloud user is obligated to rectify incorrect personal data and complete incomplete personal data upon request. The cloud provider is obligated to assist the cloud user in the rights of data

[39] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.
[40] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

subjects by means of appropriate TOMs. Rectification in accordance with Art. 16 GDPR promotes the protection goal of intervenability (SDM C1.7).

Implementation guidance

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

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

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

Reference is made to the implementation guidance in the SDM module 61 “Correction”.

Proof

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 arrange for this to be done by the cloud provider (e.g. by documentation of the relevant mechanisms and reporting channels, service descriptions). The rectifications and completions actually performed can also be verified based on process documentations and logs.

As part of an inspection, a representative sample rectification and completion can be carried out to check whether rectifications and completion of data are possible (e.g., through a technical function within the cloud service or manual requests to the cloud service support).

The cloud provider should submit records of the continuous documentation of instructions and/or software commands issued by cloud users as evidence of the execution of rectification and completion (e.g. log entries, time stamps, versioning of log files).

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

Criterion

(1) The cloud provider ensures that the cloud user itself has the possibility to perform the erasure of personal data or arrange for this to be done by the cloud provider, so that the personal data will be erased irrecoverably and no information about the data subject can be obtained from it. The cloud provider ensures that erasure is irrevocably by using state of the art measures.

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

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

(4) The cloud provider must document instructions received from the cloud user for the fulfilment of the cloud user´s obligation for granting the right to erasure or when assisting in it.

Explanation

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

Implementation guidance

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

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

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

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

Since the erasure of data in backup and fail-safe systems is more time-consuming than erasure from the active database, copies and data from backup systems can also be erased at later points in time, after the erasure from the active database, e.g. in the course of overwriting or destroying the affected data media. Erasure from the backup files should generally take place no later than one year after erasure from the active database, whereas it should generally be aimed for shorter periods. The erasure from backup and fail-safe systems should include all previous versions of the data, temporary data, metadata, and file fragments. The cloud provider can also take TOMs to perform selective erasures that will delete backups at least partially to erasure data as soon as possible.

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

Reference is made to the implementation guidance in the SDM module 60 “Erase and destroy”.

Proof

The cloud provider can demonstrate compliance with the requirements by documenting the measures for the erasure of data (e.g. documentation of the relevant mechanisms and reporting channels, erasure concepts, service descriptions). In addition, logs of instructions and subsequent erasures can be submitted.

Within the scope of an inspection, a test erasure can be executed to demonstrate that a (complete) erasure of data is possible (e.g. by means of a technical function within the cloud service or by manual inquiries with the cloud service support). As part of an audit, interviews (e.g. to gain knowledge of procedural steps, etc.) and observation can also be used to demonstrate that an erasure can be executed.

No. 6.5 – Restrictions of processing[41] (Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 18 (1) GDPR)

Criterion

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

(2) The cloud provider must document instructions received from the cloud user for the fulfilment of the cloud user´s obligation for granting the right to restriction of processing or when assisting in it.

Explanation

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

Implementation guidance

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

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

Reference is made to the implementation guidance in the SDM module 62 “Restrict processing”.

Proof

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 arrange for this to be done by the cloud provider. It can present logs of instructions and subsequent restrictions.

As part of an inspection, a test restriction can be carried out in order to demonstrate that a restriction of data processing is possible (e.g. by means of a technical function within the cloud service or through manual inquiries to the cloud service support). As part of an audit, interviews (e.g. to gain knowledge of procedural steps, etc.) and observation can also be used to demonstrate whether a restriction can be executed.

[41] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

No. 6.6 – Notification obligation regarding rectification, erasure or restriction of processing[42] (Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 19 GDPR)

Criterion

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

(2) The cloud provider must document instructions received from the cloud user for the fulfilment of the cloud user´s notification obligation in the event of restriction, erasure or restriction of processing or when assisting in it.

Explanation

In accordance with Art. 19 GDPR, the cloud user is obligated to inform recipients to whom it has disclosed personal data about any rectification, erasure or restriction of processing, and to inform the data subject of the recipients on request. If the cloud provider has been involved in the disclosure, it is obligated to assist the cloud user in fulfilling of the rights of data subjects by means of appropriate TOMs. This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Implementation guidance

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

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

Proof

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 on request or to arrange for this to be done by the cloud provider (e.g. documentation of the relevant mechanisms and reporting channels, service descriptions). It can submit logs of instructions that have been issued and subsequent notifications.

During an inspection, a test instruction for notification can be issued to demonstrate that this can be done (e.g. by means of a technical function within the cloud service or through manual inquiries to the cloud service support). As part of an audit, interviews (e.g. to gain knowledge of procedural steps, etc.) and observation can also be used to demonstrate that an instruction for notification can be given.

No. 6.7 – Data transmission[43] (Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 20 (1) and 2 GDPR)

Criterion

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

(2) The cloud provider must document instructions received from the cloud user for the fulfilment of the cloud user´s obligation for granting the right to data portability or when assisting it.

Explanation

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

[42] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

[43] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

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

Implementation guidance

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

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

Reference is made to the implementation guidance in BSI C5 PI-01 to PI-02, and COS-08.

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

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

Reference is made to the implementation guidance in the SDM module 11 “Storage”.

Proof

The cloud provider submits documentation on data transmission measures (e.g. documentation of the relevant mechanisms, export formats, service descriptions). It can submit logs of instructions and subsequent data transmissions.

Within the scope of an inspection, a test data transmission of test data can be done to demonstrate that this is possible (e.g. by means of a technical function within the cloud service or by manual inquiries to the cloud service support). As part of an audit, interviews (e.g. to gain knowledge of procedural steps, etc.) and observation can also be used to demonstrate if a data transmission can be performed.

No. 6.8 – Objection[44]
(Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 21 (1) and Art. 32 (1) lit. b) GDPR)

Criterion

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

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

(3) The cloud provider must document instructions received from the cloud user for the fulfilment of the cloud user´s obligation for granting the right to object or when assisting in it.

Explanation

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

Implementation guidance

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

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

Proof

[44] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

The cloud provider submits documentation on measures to receive objections and discontinue the processing (e.g. documentation of the relevant mechanisms and reporting channels, service descriptions). A cloud provider can submit logs of instructions issued and, if necessary, the subsequent termination of processing.

As part of an inspection, a test objection can be executed to demonstrate that the cloud provider can provide the cloud user with all data for decision-making and the processing can be discontinued if necessary (e.g. by means of a technical function within the cloud service or by manual inquiries to the cloud service support). As part of an audit, interviews (e.g. to gain knowledge of procedural steps, etc.) and observation can also be used to demonstrate if and how an objection instruction can be performed.

No. 6.9 – General obligation to inform and obligation to inform in the event of inaction or delayed request processing[45] (Art. 12 (3) and (4), Art. 28 (3) subpara. 1 lit. e) in conjunction with Art. 15 to 21 GDPR)

Criterion

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

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

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

Explanation

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

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

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

Implementation guidance

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

If instructions to fulfil the obligation to inform are implemented automatically (e.g. by means of software commands through interaction with a graphic user interface or by command line arguments), corresponding fields should also

[45] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

be provided where the cloud user can enter information about the action taken, the extension of the period, and the reasons for this or the reasons for its inaction, and the possibility to lodge a complaint with the supervisory authority or seek a judicial remedy. These user interactions should be logged automatically to demonstrate that the cloud provider acts in accordance with instructions.

Proof

The cloud provider can demonstrate compliance with the requirements by submitting documents on measures it has taken to enable the cloud user to provide information to a data subject or to arrange for the information being communicated by the cloud provider (e.g. mechanisms and reporting channels, service descriptions). Process documentation and logs can be used to prove whether the information has in fact been provided to the data subject and if it is complete.

The cloud provider should submit records of the continuous documentation of instructions and/or software commands issued by cloud users for the implementation of the provision of information (e.g. log entries, time stamps, versioning of log files) to demonstrate compliance. As part of an audit, an interview or observation of relevant employees (e.g. to gain knowledge of instructions from cloud users and guidelines for compliance with these, etc.) can be conducted for verification.

No. 7 – Assistance in data protection impact assessment[46]
(Art. 28 (3) subpara. 1 lit. f) in conjunction with Art. 35 and 36 GDPR)

Criterion

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

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

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

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

Explanation

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

Implementation guidance

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

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

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

Reference is made to the implementation guidance in the SDM module 41 “Plan and specify”.

Proof

In particular, a cloud provider should submit the documentation on obligations to inform including support documents for cloud users (e.g. service descriptions, TOMs, data flow models and analyses), performed data protection impact assessments, and corresponding meeting minutes, documentation of the precautions taken, directories of procedures, process instructions and guidelines. In particular, the cloud provider must demonstrate that the necessary information is available or that it can be generated by the cloud provider within a short period of time.

[46] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

An interview of relevant employees as part of an audit (e.g. to gain knowledge of guidelines, etc.) can be submitted as evidence. Observations can be used to demonstrate whether and how the cloud provider's employees process a test request to assist in a cloud user's data protection impact assessment.

Chapter III: Data protection management system of the cloud provider

Explanation

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

No. 8 – Data protection management system

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

Criterion

(1) The cloud provider must designate a data protection officer (DPO) where its core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.

(2) The cloud provider must designate a DPO where its core activities consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

(3) The cloud provider must designate a DPO if its constantly employs as a rule at least 20 persons dealing with the automated processing of personal data.

(4) The cloud provider must designate a DPO if it undertakes processing subject to a data protection impact assessment pursuant to Article 35 GDPR, regardless of the number of persons employed in processing.

(5) The cloud provider must designate a DPO if it commercially processes personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research, regardless of the number of persons employed in processing.

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

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

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

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

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

(11) The cloud provider must ensure that the DPO is able to carry out his tasks in accordance with Art. 39 (1) GDPR to an appropriate extent, including informing and advising, monitoring compliance, and cooperating with and acting as the contact point for the supervisory authority.

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

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

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

Explanation

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

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

According to section 38 para. 1 of the Federal Data Protection Act (BDSG) the controller and processor are obligated to designate a data protection officer if they constantly employ as a rule at least 20 persons dealing with the automated processing of personal data.

They shall also designate a data protection officer regardless of the number of persons employed in processing, if the controller or processor undertake processing subject to a data protection impact assessment pursuant to Article 35 of Regulation (EU) 2016/679, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research.

Implementation guidance

The cloud provider should document its elaboration whether a DPO must be designated, including the conditions assessed in accordance with (1) – (4) and the assessment results for each condition.

The cloud provider should maintain written documentation of the systems, procedures and processes (software, hardware, involved organisational units, roles, and service providers) used for the cloud service in question and provide as accurate a description as possible of all TOMS put in place (e.g. in a data security program), and make this available to the DPO and, upon request, to the supervisory authority. The cloud provider should establish TOMs to ensure that the DPO is consulted early on in the cloud development process that may lead to changes in data processing. For example, a ticket system can be used to involve the DPO.

If the DPO is employed by another company (external DPO of the cloud provider) or if he is simultaneously also the DPO of other companies, the DPO's independence from instructions also applies to its employer and other clients. The requirement of the absence of conflicts of interest is primarily a designation requirement and, in a secondary respect, an organisational obligation of the cloud provider. The cloud provider does not assign additional tasks to the DPO which could result in a conflict of interests. Conflicts of interest are to be assumed present in the course of the following activities: activities within the scope of which the DPO would have to monitor himself, e.g. position as a managing director, IT or HR manager, economic interests of the DPO in the success of the company or in too close a proximity to the designating body.

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

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

Proof

The cloud provider can demonstrate compliance with the requirements by designating a DPO and reporting the contact details of the DPO to the competent supervisory authority and presenting him to the public as the contact person on its website. Internal documents such as the submission of the DPO's job description or designation certificates, certificates of professional competence (e.g. certificates, training certificates), descriptions of tasks and procedures, guidelines, or organisational charts that describe the DPO's attribution can be suitable evidence. The same applies to the provision of logs on employee information on the role of the DPO, to minutes of meetings with the DPO to check the fulfilment of requirements and to activity report'.

The cloud provider can submit relevant certificates and evaluations toassess the DPO's professional and personal qualification. An interview of the DPO during an on-site audit can also provide information about his qualification and position in the company. An on-site audit can also demonstrate that the DPO is provided with the necessary resources and support.

To assess the obligation of secrecy or confidentiality, the cloud provider can submit the corresponding signed designation certificate with the required content.

The DPO's activities, independence, involvement, and effectiveness in the cloud provider's organisational structure can be demonstrated in internal audits to be conducted at regular intervals. The relevant audit protocols should be submitted for review. Logs and other documents as well as an interview with the management can be used as verification for whether the DPO reports directly to the highest management level. An interview of the DPO about his tasks is suitable to demonstrate that he is not subject to any conflict of interest. In addition, documents informing about the hours worked by the DPO can be submitted.

No. 8.2 – Notification of personal data breaches[47]
(Art. 33 (2) and Art. 28 (3) subpara. 1 sent. 2 lit. f) GDPR)

Criterion

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

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

(3) The responsible departments or persons in the cloud provider´s organisation must have sufficient resources to ensure that notifications are processed without undue delay. The employees in the responsible departments must be sufficiently trained to be able to assess violations and carry out an impact assessment.

Explanation

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

Implementation guidance

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

Reference is made to the guidelines 9/2022 on personal data breach notification under GDPR.

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

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

Proof

A cloud provider submits the data security program and the TOMs described therein to ensure that personal data breaches are notified. It can also submit further documentation on information and notification obligations, including, for example, process documentation for informing users, directories of procedures, procedural instructions, guidelines and training documents.

The implementation of this concept can be proven by via an inspection or observation of a test notification of a personal data breach for a simulated cloud user. Logs of past notifications of personal data breaches to users can also serve as proof of the requirements. It should be demonstrated in the course of an on-site audit that sufficient resources are available to ensure that notifications are processed promptly.

The competence of the employees should be demonstrated by records verifying their skills such as certificates or training courses and by means of employee interviews. An organisational chart or an overview of the personnel situation in responsible areas with appropriately documented personnel qualifications can also be presented. Interviews can also be used to demonstrate that responsibilities are defined and communicated clearly (e.g. as to who is responsible to decide whether to notify the personal data breach to the cloud user and who implements the notification).

[47] This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

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

Criterion

(1) The cloud provider must maintain a record of processing activities if it employs 250 or more persons.

(2) The cloud provider must maintain a record of processing activities if the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects.

(3) The cloud provider must maintain a record of processing activities if the processing is not occasional.

(4) The cloud provider must maintain a record of processing activities if the processing includes special categories of data as referred to in Article 9 (1) GDPR or personal data relating to criminal convictions and offences referred to in Article 10 GDPR.

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

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

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

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

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

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

Explanation

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

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

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

Implementation guidance

The cloud provider should document its elaboration whether a records of processing activities must be maintained, including the conditions assessed in accordance with (1) – (4) and the assessment results for each condition.

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

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

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

Reference is made to the implementation guidance in the SDM module 41 “Plan and specify” and module 42 “Documentation”.

Proof

The cloud provider submits the records of processing activities and demonstrates that they are complete and up to date (e.g. time stamp, versioning history). If a standardised legally binding Commissioned Data Processing Agreement has been concluded with the cloud user, the underlying standardised records of processing activities are to be submitted. If no standardised legally binding Commissioned Data Processing Agreement s have been concluded with a cloud user, a cloud provider submits all or a representative sample of records of processing activities of cloud users. Employee interviews can be carried out conducted to assist in the process of an audit for the purpose of verifying that the records are complete and up to date.

The cloud provider submits process documentation regarding the updating of the records of processing activities and regarding the cooperation between the parties involved in preparing the records of processing activities. Process documentation for receiving, processing and answering requests from supervisory authorities regarding records of processing activities should also be submitted. Organisational charts, task distribution plans or other documents can be submitted as proof of regulated responsibilities. Furthermore, as part of an audit, employee interviews can be carried out to prove that the defined processes are known and practiced at the company. The cloud provider can prove the representative's current and complete records of processing activities likewise by submitting them.

No. 8.4 – Return of data media and erasure of data; demonstrating compliance and allowing for and contribute to audits
(Art. 28 (3) subpara. 1 sent. 2 lit. g) and h) GDPR)

Criterion

(1) The cloud provider must ensure by appropriate measures that the return of provided data media (containing personal data), the return of personal data, and erasure of personal data stored by the cloud provider take place after the completion of the processing on the behalf of the cloud user or upon instruction by the cloud user, unless Member State or Union law prescribe an obligation for the storage of the personal data. This criterion would not apply to the cloud user falling under the household exemption. The cloud provider as a processor is well advised to treat the criterion as existing and potentially to be fulfilled in order to be able to react to such changes in the role of a cloud user becoming a controller.

(2) The cloud provider must ensure by appropriate measures that it is able to provide all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Implementation guidance

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

Since the erasure of data in backup and fail-safe systems is more time consuming than erasure in the active database, copies and data from backup systems can also be erased at later times than in the active database, e.g. in the course of overwriting or destroying the affected data media. Erasure in the backup files should take place usually no later than one year after erasure from the active database, whereas shorter periods should be generally aimed for. Erasure in backup and fail-safe systems should include all previous versions of the data, temporary data, metadata, and file fragments. The cloud provider can also take TOMs to perform selective erasures that will delete backups at least partially to erasure data as soon as possible.

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

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

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

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

Reference is made to the implementation guidance in BSI C5 AM-04, AM-05, and PI-03.

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

Reference is made to the implementation guidance in the SDM module 11 “Storage” and module 60 “Erase and destroy”.

In regard to demonstrating compliance and allowing for and contribute to audits, reference is made to the implementation guidance in the EU Cloud CoC Section 5.5 “Right to audit”.

Proof

The cloud provider can demonstrate compliance with the requirements by submitting documents that describe its procedures for the handover of the data media, the return and erasure of the data after the contract has ended. Regarded as suitable documents are the records of TOMs, data erasure concepts, directories of procedures, process documentation for data (media) handling, procedural instructions, guidelines, or documented instructions. It can also submit the confirmations of returns or the automated notification of actual erasures of the personal data that are no longer necessary for the commissioned data processing.

By means of inspection and/or test (e.g. source code analysis or analysis of databases) or a test erasure and return, it can be demonstrated whether personal data is erased and returned after the commissioned processing has been completed or the cloud user has given an accordant instruction. An interview of relevant employees in the course of an audit (e.g. to gain knowledge of guidelines etc.) can serve as further proof of the implementation of the measures. Security tests can be carried out as further support to demonstrate that data have been erased with sufficient security.

The cloud provider can submit appropriate documentation verifying that the cloud provider actively undertakes means to make information available as needed in Art. 28 GDPR and allows for and contributes to audits carried out by the controller or other auditors mandated by it.

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

Criterion

(1) The cloud provider must review the implementation of all criteria examined in this catalogue regularly (at least annually, and after each major change) in an internal audit procedure. For this purpose, the cloud provider must define control procedures and responsibilities, and act upon audit findings with preventive and corrective actions.

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

Explanation

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

Implementation guidance

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

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

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

Reference is made to the implementation guidance in BSI C5 DEV-01 to DEV-10 with regard to the embedding of the audit process in the change management and COM-01 to COM-4.

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

Proof

The cloud provider submits documentation for the implementation of audits (e.g. TOMs, directories of procedures, procedural instructions, guidelines, role descriptions, audit and result protocols or schedules for internal audits). Whether internal controls are being carried out can be demonstrated by interviewing the DPO, the responsible employees and management as part of an audit. In particular, it should also be demonstrated that employees are aware of their assigned and documented responsibility, and that they perform their tasks with regard to the execution of control procedures.

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

Criterion

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

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

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

Explanation

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

Implementation guidance

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

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

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

Proof

The cloud provider can demonstrate compliance with the required know-how of its employees by means of relevant qualification documentations (e.g., certificates, documentation on qualification requirements, training documents, evidence of participation, role and authorisation descriptions and concepts, procedural instructions and guidelines). 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.

The establishment of the implementation of the rules can be proven in the context of an on-site audit (e.g. clean desk principle, screen locks) and interviews of the employees (e.g. examination of know-how, awareness of the guidelines, potential conflicts of interest).

Chapter IV: Data protection by system design

No. 9 – Data protection by design and by default

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

Criterion

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

(2) The cloud provider must maintain processes to be able to show that personal data are processed in a transparent manner in relation to data subjects (principle of transparency). It must further maintain processes for an active monitoring of its compliance with the implementation of state of the art TOMs, regarding all levels of the conceptual objectives[48] of its services offered, their architectures and their system designs.

(3) The cloud provider must ensure at all times that its system design in the offered applications and the service concept guarantee the traceability (while considering data minimization, refer to No. 2.6 [1]) and transparency of the data processing, even when service chains are extended by potential sub-processor relationships.

Explanation

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

Implementation guidance

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

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

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

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

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

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

[48] Conceptual objectives are those that aim at the relevant model of the services offered, i.e. offering software, platforms, or infrastructure services etc.

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

Reference is made to the implementation guidance in the SDM module 41 "Plan and specify", module 42 "Documentation", and module 51 "Control access to data, systems and processes".

Proof

A cloud provider can carry out a large number of measures to demonstrate compliance with data protection by system design.

The cloud provider can submit documents showing which risks it has addressed and which design principles and measures it has determined to minimise the identified risks and implement the data protection principles. The documentation should also include the considerations, which have guided the cloud provider in the choice of TOMs. Relevant documentation includes service descriptions, the data security program with the TOMs, role and authorisation concepts, process descriptions, procedural instructions, guidelines, template contracts for sub-processors, result logs of internal audits and sub-processor controls, risk analyses, documentation of the information security management system, incident response management documentation and data protection impact assessments.

The comparison of the documentation to the actual implementation of the measures should be verified by inspections and (on-site) audits. As part of an inspection, a trial use of the service (e.g. check of functions and measures according to the service description), process monitoring (e.g. ensuring encryption) and an asset tests (e.g. source code analysis, analysis of system interfaces and hardware components) can be carried out to demonstrate compliance with the implementation of the data protection principles for the hardware or software that is used and the implementation of the data processing operations. An employee interview or observation of relevant employees should also be carried out to prove their knowledge of guidelines and procedural steps, as well as their competencies and responsibilities. In addition, the management should be interviewed to demonstrate that data protection by system design is a firmly rooted objective of the company and explain the decision-making processes and considerations that are made.

A development and design review can be carried out to demonstrate that the data protection requirements have been considered already during the phase of system development. For this purpose, the cloud provider can submit documents on the development methods and procedures that were employed (in particular, acceptance criteria and lists of requirements). If necessary, test systems and environments can be inspected (e.g. for appropriateness and security). During the design review, documentation can be submitted relating to the selected architecture, database diagrams, data flow diagrams, design decisions, as well as the configuration and settings of the cloud service for providing the data processing operation.

The cloud provider proves that the state of the art is observed and met by means of process documentation (e.g. logs of decisions, time stamps, versioning history, and change logs) and employee interviews (e.g. awareness of the guidelines and separation of responsibilities).

Security tests can be used, for example, to be able to prove the security and appropriateness of design measures.

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

Criterion

(1) The cloud provider must ensure by default settings in the respective services that only personal data that are necessary for the relevant purpose of the processing are processed in regard to the amount of personal data collected, the extent of their processing, and the period of their storage and that personal data are only accessible to the extent necessary to fulfil the processing purpose of the cloud user[49].

(2) The cloud provider must ensure by default that personal data are not made accessible without the individual's intervention to an indefinite number of natural persons and that no inappropriate risks[50] arise for the data subject from providing in a too expansive extent[51] access to personal data available.

Explanation

[49] In regard to the latter the cloud provider must ensure that persons acting under its authority shall access the personal data only on a need to know basis.
[50] Inappropriate risks arise from not taking 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 natural persons posed by the processing.
[51] A "too expansive extent" is given if a technical or personal access grants more information as is necessary for the relevant purpose of the processing.

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

Implementation guidance

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

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

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

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

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

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

Reference is made to the implementation guidance in the SDM module 41 “Plan and specify”, module 42 “Documentation”, and module 51 “Control access to data, systems and processes”.

Proof

A cloud provider can carry out a large number of measures to demonstrate compliance with data protection by default.

The cloud provider submits documents that describe which default settings have been selected and for what reasons. The documentation of the individual TOMs, the data security program, standard settings of the cloud service, procedural instructions, guidelines and/or concepts for passwords, authentications, and admission and access authorisations can be presented. Documentation on the separation of test systems, the development of the cloud service and protocols and other evidence for the implementation of technical default settings can also be submitted.

The actual implementation of the measures should be proven by means of inspections, tests and (on-site) audits. In the course of an inspection, a trial use of the service (e.g. checking the standard values and preselection of data fields), process monitoring (e.g. implementing the measures to separate the development systems) and an asset test (e.g. source code analysis, analysis of system interfaces and hardware components) can be carried out to prove the default settings. An employee interview or observation of relevant employees should also prove their knowledge of guidelines and procedural steps, and the provided awareness-raising training as regards data protection and data security, in addition to their competencies (especially with regard to the necessity of processing data). The management should be interviewed to demonstrate that data protection by default is a firmly rooted objective of the company.

A development and design review can be carried out to prove that the data protection requirements and default settings have been considered already during the phase of system development. For this purpose, a cloud provider can submit documents on the development methods and processes that were employed (in particular, acceptance criteria and selected default settings). If necessary, test systems and environments can be inspected (e.g. for appropriateness and security). During the design review, documentation can be submitted relating to the selected architecture, database diagrams, data flow diagrams, design decisions, as well as the configuration and settings of the cloud service for providing the data processing operation.

Security tests can be used, for example, to be able to prove the security and appropriateness of design measures.

Chapter V: Sub-processing

Explanation

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

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

No. 10 – Sub-processing relationships

No. 10.1 – Further processors of the cloud provider (sub-processing) (Art. 28 (2, 4) GDPR)

Criterion

(1) The cloud provider must have a defined process, which ensures that a cloud service is provided with the involvement of sub-processors only if and insofar as the cloud user has given its prior specific or general authorisation for this sub-processing. The authorisation must be given in writing or in an electronic form. In the case of general written authorisation, the cloud provider must inform the cloud user of any intended changes concerning the addition or replacement of other processors, thereby giving the cloud user the opportunity to object to such changes.

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

(3) The cloud provider must ensure that all the sub-processors it engages will implement the TOMs defined by the cloud provider during its risk assessment or required by the certification criteria. The cloud provider must further ensure that the same obligations as set out in the Legally Binding Commissioned Data Processing Agreement or any other legal act between itself and sub-processors are imposed to any link of the chain of sub-processors.

Explanation

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

Since the right to object to changes in subcontracted processing must not be devalued in practice, any contractual obligations from the legally binding Commissioned Data Processing Agreement addressing the prerequisites and consequences of an objection to sub-processors must be taken into regard concerning contractual obligations with relevant sub-processors at all levels of the commissioned data processing.

Implementation guidance

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

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

Reference is made to the implementation guidance in BSI C5 OIS-03, SSO-01 to SSO-05.

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

Proof

The cloud provider can demonstrate legal compliance with further data processing by submitting the authorisation given by the cloud user. The specific authorisation given contains the identities of the authorised sub-processors, their addresses, the descriptions of the activities that they are to perform, and a delimitation of the responsibilities between the cloud provider and the sub-processor(s) and between different sub-processors. In addition, contracts for further commissioned data processing (sub-cloud contracts) can be submitted together with the information required for the document review (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 for sub-processing (Art. 28 (4) GDPR)

Criterion

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

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

Implementation guidance

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

Proof

The cloud provider can demonstrate that the further data processing is legally compliant by submitting the legally binding Commissioned Data Processing Agreement and the legally binding data sub-processing agreement, together with the information required for the document review (duration, type and purpose, place of further processing, information on the additional processor and its service description).

The cloud provider can submit the list of involved sub-processors in order to enable a check of concluded sub-processing-agreements. The cloud provider should submit documents of the TOMs, the data security program or certificates for the respective sub-processors. Other relevant documents can be used for demonstrating compliance, including the template contract with sub-processors on commissioned data processing, guidelines and instructions, further safeguards of the sub-processors, internal control areas of the cloud provider relating to sub-processor controls, the data protection concept or the risk assessment in case of subcontracting.

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

Criterion

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

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

Explanation

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

Please also refer to criteria No. 1.5 and No. 4.2.

Implementation guidance

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

Information platforms within or outside the offered cloud service are suitable for showing which sub-processors are involved and proactively inform ("push"-information) cloud users of changes in sub-processing. They should be maintained and updated on a continuous basis.

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

Proof

The cloud provider can demonstrate its compliance with the requirements by submitting documents (such as specific legally binding sub-processing-agreements or templates of such agreements) wherein cloud users are advised of how they will be informed in the event of intended changes of sub-processors (e.g. by email or in information portals). In addition, the cloud provider should provide documentation on how objections from cloud users are received and processed. Further relevant documents for demonstrating compliance can be, for example, documentation of the consents of cloud users and documentation relating to the exercise of the right to object. Logs of notified changes in the involvement of sub-processors or processed objections should be submitted by the cloud provider, if these happened.

In addition, the cloud provider can submit its detailed documentation on the involved sub-processors, stating their identity, summons address and the performed processing operations, by means of which it is possible to track which (sub-) processor performs which processing operations.

An inspection in the form of process monitoring or an observation in the course of an audit can be used as proof of the information required for the involvement of sub-processors are communicated appropriately to the cloud user. For this purpose, information about the change of a sub-processor can be simulated as a test. Likewise, the processing of an objection by a cloud user can be verified. An interview of relevant employees (e.g. knowledge of guidelines, receipt of inquiries and objections from the cloud user, etc.) can serve as further proof.

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

Criterion

(1) The cloud provider must ensure that at all levels, sub-processors are only involved if they offer a guarantee of compliance with the data protection obligations set out in the legally binding Commissioned Data Processing Agreement for the service they are providing.

(2) The cloud provider must satisfy itself of all hired sub-processors fulfilling the data protection obligations set out in the legally binding Commissioned Data Processing Agreement for the services they are providing.

Implementation guidance

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

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

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

Proof

The cloud provider can prove its compliance with the requirements by submitting certificates of the sub-processors or other documents (e.g. codes of conduct they follow, legally binding sub-processing-agreements, data security programs, further safeguards) that guarantee compliance with the General Data Protection Regulation. A transparent service description of the respective sub-processor can be helpful. In addition, documents on the selection (e.g. records of selection considerations and decisions) and the implementation of internal controls (e.g. records of the sub-processor controls) can be useful for demonstrating compliance with the requirements.

As support, employee interviews (e.g. regarding the familiarity with procedural steps and safeguards of the subcontracted processors) can be part of an audit to find out how compliance with data protection requirements is verified by sub-processors.

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

Criterion

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

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

Implementation guidance

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

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

Proof

The cloud provider submits documents on procedures and precautions applied when sub-processors are engaged so as to demonstrate compliance with the requirements, including legally binding agreements with sub-processors, process documentation relating to the involvement, data security programs and information about contact persons at the sub-processors, risk analyses or documents for the separation of responsibilities for the individual processing operations. Protocols for the fulfilment of obligations in consequence of the involvement of other processors can be submitted.

As proof, an interview of employees can be performed concerning the involvement of sub-processors (with regard to the familiarity of procedural steps and contact persons of the sub-processors).

If available, TOMs used by the cloud provider to automatically monitor sub-processors' data processing should be audited (e.g., SIEM systems, or offered APIs by sub-processors).

Chapter VI: Processing outside of the EU and EEA

No. 11 – Data transfers[52]

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

Criterion

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

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

(3) If, after assessing law and practice of the third country, the appropriate safeguards within the meaning of Art. 46 (2) or 3 GDPR as specified under the legally binding Commissioned Data Processing Agreement[53] prove to be insufficient for ensuring an adequate level of protection equivalent to that of the General Data Protection Regulation, the cloud provider must take supplementary measures to ensure this adequate level of data protection. Otherwise, the data transfer must not take place. The cloud provider must provide for a cloud user to receive the assessment carried out, with regard to the law and practice of the third country, so as to verify whether the supplementary measures adopted by the processor effectively ensure an adequate level of protection of the personal data transferred in the third country.

(4) The cloud provider must continuously monitor the adequacy of the level of data protection and ensure that data transfers are immediately suspended or terminated if, in the case of para. 2 or 3, the recipient has infringed the obligations it has entered into under the appropriate safeguards of Art. 46 para. 2 or 3 GDPR or its fulfilment is impossible and in the case of para. 3 the supplementary measures can no longer be complied with or are ineffective. [54]

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

(6) Whenever the cloud provider transfers data (within the meaning of Art. 44 GDPR) to a processor established outside the EU or the EEA, the cloud provider must fully respect the obligations stipulated in Chapter V of the GDPR.

Explanation

Transfers of personal data of data subjects to third countries are only permitted under the conditions set out in Art. 44 et seq. GDPR. The same applies to the transfer of personal data to an international organisation for which no adequate level of data protection is recognised. It is essential, that the processor needs to act in accordance with the instruction of the controller.

If the commissioned data processing includes the instruction for a data transfer to third countries or international organisations, Art. 44 GDPR also requires compliance with the requirements of Chapter 5 GDPR. It should be noted

[52] Transfer refers to the movement of personal data when it is transferred from the EU/EEA to a country or countries outside the EU/EEA and also cases where data is made accessible through remote access or disclosed to the data importer. See EDPB Guidelines 05/2021 on Interplay between Art. 3 and Chapter V of GDPR.

[53] It is self-understanding that the processor is still bound to act in accordance with the instructions of the controller in regard to data transfers as given by the legally binding Commissioned Data Processing Agreement, see criterion no. 1.4(1).

[54] It is self-understanding that the processor is still bound to act in accordance with the instructions of the controller in regard to data transfers as given by the legally binding Commissioned Data Processing Agreement, see criterion no. 1.4 (1).

that the regulation of Art. 49 GDPR does not contain any permissions for the systematic and regular data transfer between exporter and importer[55], as it is customary in cloud computing. Systematic and regular data transfers between exporter and importer must therefore be based on adequacy decisions pursuant to Art. 45 (3) GDPR or the appropriate safeguards pursuant to Art. 46 (2) or (3) GDPR, which have been determined between the cloud provider and the cloud user in accordance with no. 1.4. Data transfers on the basis of Art. 49 GDPR may take place, if at all, only in very restrictive exceptional cases which, however, are not covered by this Criteria Catalogue.

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

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

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

A possibility for the controller must exist to receive the assessment carried out with regard to the law and practice of the third country so as to verify whether the supplementary measures adopted by the processor effectively ensure an adequate level of protection of the personal data transferred in the third country.

It is self-understanding, that the legally binding Commissioned Data Processing Agreement will still have to be complied with in regard to data transfers as is laid down in no. 1. 4 (1).

Implementation guidance

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

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

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

[55] Data exporter is/are the natural or legal person(s), public authority/ies, agency/ies or other body/ies ("entity/ies") transferring the personal data to a third country. The entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity is/are the data importer, see Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

The following legal provisions, which implicitly or explicitly regulate legal powers of public authorities to access personal data, can be taken into account for the assessment of law and practice in the following countries, whereby this list is exemplary and not exhaustive in relation to the countries and the legal provisions[56]:

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

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

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

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

2. Russia: Federal Law on “Foreign Reconnaissance” of 10.1.1996 No. 5-FZ (Федеральный закон от 10.1.1996 г. N 5-ФЗ "О внешней разведке"), Federal Law on “the Federal Security Service” of 3.4.1995 (Федеральный закон "о федеральной службе безопасност" от 03.04.1995 г. N 40-ФЗ), Federal Law "on operational search activities" of 08.12.1995 No. 144-FZ (Федеральный закон "Об оперативно-розыскной деятельности" от 08.12.1995 г. N 144-ФЗ), Federal Law "on Communication" of 7.7.2003 No. 126-FZ (Федеральный закон "О связи" от 7.7.2003 г. N 126-ФЗ). These regulations permit public authorities to use companies from Russia for intelligence purposes and to force them to disclose personal data.

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

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

- The case law of the ECJ such as the Schrems II judgment for the USA or the case law of the European Court of Human Rights (ECHR) such as the factsheet on mass surveillance;
- Adequacy decisions for the third country if the data transfer relies on a different transfer instrument;
- Resolutions and reports of intergovernmental organisations such as the Council of Europe or regional bodies, e.g. the country reports of the Inter-American Commission on Human Rights or United Nations organisations like the Human Rights Council or the Human Rights Committee of the United Nations;
- Reports and analyses of competent regulatory networks such as the Global Privacy Assembly (GPA);
- National case law or decisions taken by independent judicial or administrative authorities competent on data protection and the protection of privacy of third countries;
- Reports of independent oversight or parliamentary bodies;
- Reports based on practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, from entities active in the same sector as the recipient;

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

- Warrant canaries[57] of other entities processing data in the same sector as the recipient;
- Reports produced or commissioned by Chambers of commerce, business, professional and trade associations, governmental diplomatic, trade and investment agencies of the exporter or other third countries exporting to the third country to which the transfer is made;
- Reports from academic institutions, and civil society organizations (e.g. NGOs).

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

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

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

The four European Essential Guarantees are:

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

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

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

   In accordance with Art. 52 (1) sent. 1 CFR (Charter of Fundamental Rights of the European Union), any limitation of the rights recognised by the Charter must respect the essence of these rights, which is why limitations through access measures may only be made if they are necessary while maintaining the principle of proportionality and if they genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The assessment of whether a limitation is proportionate depends, on the one hand, on the severity of the interference entailed by a limitation and, on the other hand, whether the public interest objective pursued by the limitation is proportionate to the severity of the interference. For example, access by public authorities to the location of a data subject's mobile phone in real time is a serious interference because it enables the public authority to track the movements of the data subject at any time. However, it could be proportionate if it aims, e.g. at preventing imminent, serious acts of terrorism or searching for injured or missing persons. The limitation of a right

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

must be limited to what is strictly necessary, which presupposes that for the access measures it must be precisely regulated by legal provisions when, under which circumstances and conditions the access measures may be used and what minimum safeguards must be observed by the public authority. Legal provisions that allow interferences within the meaning of access measures to personal data by public authorities without providing limitations, do not meet the requirements for an equivalent level of data protection, since every legal provision for an interference must define the scope of the limitation of the respective rights. Furthermore, the principle of necessity is not complied with if legal provisions for access measures disrespect the essence of rights. This is the case, e.g. regarding Art. 7 of the Charter if public authorities are permitted under legal provisions to generally access the content of electronic communication without the interference being limited, the objectives pursued by the interference being named and objective criteria for the use of the access measure being defined.

3. Independent oversight mechanism

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

4. Effective remedies

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

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

According to Article 28(3)(a) GDPR, the controller must be provided by the processor with the assessment it has carried out with regard to the law and practice of the third country so as to verify whether the supplementary measures adopted by the processor effectively ensure an adequate level of protection of the personal data transferred in the third country. It is self-understanding that the processor is still bound to act in accordance with the instructions of the controller in regard to data transfers as given by the legally binding Commissioned Data Processing Agreement, see criterion no. 1.4(1), therefore a transfer can only take place on the instruction of the controller.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Use case: Data transfer to a cloud service that requires access to unencrypted data due to the type of commissioned data processing. If the law of a third country applies to the recipient, which grants public authorities access to personal data that goes beyond what is necessary and proportionate in a democratic

society, technical measures such as transport encryption during transfer and the encryption of personal data at rest is not sufficient to protect the rights of the data subjects. The combination of the named technical measures with supplementary contractual measures such as the contractually guaranteed obligation of the importer to challenge the requests of disclosure received from public authorities and to pursue legal recourse in the national courts against a disclosure request or the contractual obligation to inform the exporter of any disclosure requests received before the data are transferred to the public authority is not sufficient to legitimate a data transfer to the third country in question. **In use case 3, no data transfer should therefore take place.**

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

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

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

Proof

The cloud provider can demonstrate compliance with the requirements by submitting a list of sub-processors from third countries with an adequacy decision in accordance with Art. 45 (3) GDPR.

If there is no adequacy decision, documents that contain the agreed appropriate safeguards in accordance with Art. 46 (2) or (3) GDPR can be used for demonstrating compliance (e.g. standard data protection clauses, binding corporate rules in accordance with Art. 47 GDPR).

In addition, in this case, documentation from the cloud provider must be submitted to assess law and practice of the relevant third country based on the six-step roadmap. The documentation of step 3 of the roadmap has to show which sources of information the cloud provider has used to assess law and practice of the third country. First of all, the cloud provider must disclose which specific legal regulations of the third country it has considered so as to assess law and practice of the third country. The cloud provider's documentation has not only to address the legal regulations but also has to include other sources of information, if available, such as relevant decisions by the ECJ, statements and reports from intergovernmental organisations, national case law or decisions by independent judicial or administrative authorities with responsibility for the protection of privacy and data protection in third countries, reports from research institutions and civil society organizations, etc. The cloud provider’s documentation of the legal practice in the third country can also include statistics from the recipient or its partners regarding the access of public authorities to personal data as well as generally accessible sources of information such as articles from reputable newspapers that deal with the application of the relevant legal regulations by the public authorities. The documentation of the cloud provider must show why it has concluded that the instrument used for data transfer pursuant to Art. 46 (2) or (3) GDPR is sufficient to ensure an adequate level of protection. It is also important that the documentation provided shows how the four European Essential Guarantees are complied with in the third country concerned. For this reason, detailed explanations have to be provided of these individual guarantees and how they interact. Furthermore, as part of an audit, an interview of employees who are entrusted with the assessment of the law and practice of the third country, will be carried to find out how information about the third country is obtained and how law and practice are analysed and assessed with regard to compliance with the European Essential Guarantees.

If supplementary measures are necessary to ensure an adequate level of protection in the third country, the cloud provider shall submit documentation on the supplementary measures having been taken in accordance with step 4 of the roadmap. If, for example, pseudonymisation or encryption is used, it submits documentation on the respective procedures, which also shows that state-of-the-art procedures are employed and the encryption or pseudonymisation is applied before the data transfer to the recipient. In addition, the encryption must demonstrate that the keys are properly managed and remain with the exporter. Technical measures can also be demonstrated by means of technical tests or inspections. Supplementary contractual measures must be demonstrated by submitting corresponding contracts with the recipients. If supplementary organisational measures are guaranteed

in the contract, these can be demonstrated, depending on the type of the organisational measure, by submitting, e.g. transparency reports or "warrant canaries" received from the recipient.

The cloud provider can submit further documents on measures that are used to regularly assess the adequacy of the level of protection in the third country, e.g. proactive inquiries from recipients about legal changes in the third country concerned, processing of the regular reports that the recipient makes to the cloud provider due to contractual obligations about legal provision changed or requests from public authorities. Furthermore, documentation should be submitted on measures, procedures and responsibilities taken by the cloud provider if the level of protection in the third country is no longer adequate and data transfer is therefore terminated. Here, too, an interview can be carried out for Proof as part of an audit with the responsible employees, e.g. with regard to knowledge of the relevant procedure in this case.

A currently valid certification according to Art. 42 (2) GDPR, which has already been obtained for data processing operations for the object of certification to be certified, can also be used as proof. In this case, the commitments made to apply the appropriate safeguards are also to be disclosed and to be verified.

If the cloud provider processes personal data and is not only subject to the law of the General Data Protection Regulation, but also to the law of a third country, which obligates it to disclose this personal data to public authorities of the third country concerned, it has to submit documents about the supplementary measures that it has taken to effectively protect the personal data from disclosure to the public authorities of the third country. If, e.g. the cloud provider is contractually obligated to the cloud user to have refrained from intentionally including back doors or similar in the cloud service that would allow the public authorities of the third country to access the personal data, and contractually obligated that it does not intend to do so either and is also not obligated to do so under the law of the third country, it should disclose the corresponding clauses of the contract. If, e.g. pseudonymisation or encryption is used as technical measures, the cloud provider has to submit documentation on the respective procedures, which also shows that procedures according to the state of the art are used. Technical measures are also to be demonstrated by technical tests or inspections. Furthermore, documentation on the procedure and responsibilities are to be submitted in the event that the cloud provider is obligated to disclose personal data to public authorities of third countries. An interview with the responsible employees in the course of an audit, e.g. with regard to knowledge of the specified procedure, can serve as proof.

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

Criterion

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

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

Implementation guidance

The cloud provider can decide whether the representative should act in addition to the cloud provider or as the sole contact person; this is to be communicated accordingly in relation to third parties. If the cloud provider does not have an establishment in the EU or the EEA and offers its service in several Member States, it does not have to appoint a representative in each Member State, instead it can appoint a representative in a Member State with responsibility for several Member States, provided that there are data subjects in this Member State.

Proof

A cloud provider can submit various documents as proof of compliance with the requirements, including contracts with representatives, the written designation certificates, guidelines, public information for cloud users (e.g. contact information of the representative in the privacy policy on the website), responsibilities and descriptions of their roles. An interview of the representative or representatives (including on a random basis) can be conducted.

D. Criteria and implementation guidance for processing as a controller

Chapter VII: The cloud provider as the controller

Explanation

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

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

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

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

Criterion

(1) The cloud provider must provide the data subject with all information it needs to verify the lawfulness of the processing of personal data, which are required for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations (principle of transparency and lawfulness). The cloud provider may only process the data subject's data in a fair manner (principle of fairness[58]).

(2) The cloud provider must define the purposes of each data processing clearly and precisely for the performance of the contract on the provision of the cloud service and fulfilling legal obligations (principles of purpose specification and purpose limitation).

(3) The cloud provider must define a process and it has put TOMs in place that ensure that personal data are processed only insofar as it is necessary (i.e., adequate, relevant and limited to the necessary extent) to achieve the specified purposes of the processing (principle of data minimisation).

(4) The cloud provider must define a process and it has put TOMs in place for verification of the factual accuracy, rectification, and erasure of inaccurate or incomplete personal data, which it processes for performing the contract on the provision of the cloud service and to fulfil legal obligations (principle of accuracy).

(5) The cloud provider must define a process and ensure by means of TOMs that data subjects can be identified during the data processing only for as long as this is necessary for achieving the specified purposes of the performance of the contract on the provision of the cloud service or the fulfilment of legal obligations, and must delete data that are no longer necessary as soon as possible. For this purpose, it

[58] ""Fairness" can be seen as a kind of catch-all clause "in order to be able to qualify data processing that is objectionable as unclear as unlawful even in the absence of a relevant regulation". This legal term is already occupied by German civil law and there refers to "good faith" and the element of trust into performing a duty by the obligor due to a justified expectation. Regarding personal data processing, the processing may be understood as unfair if it abuses trust. Justified trust can be induced explicitly through agreements or previous behaviour or implicitly through legitimate expectations of compliance with traffic, commercial or professional rules. Trust is also abused if consent is requested even though data processing is permitted by law." The principle of fairness must be taken into account e.g. "when weighing up the conflicting interests between the controller and the data subject in accordance with Art. 6 para. 1 subpara. 1 lit. f, when determining the voluntary nature of consent and the prohibition of tying in accordance with Art. 7 para. 4, and when defining rules of conduct in accordance with Art. 40 para. 2.", see Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 5, recital 47.

sets criteria according to which the identification of data subjects is determined, maintained for the specified purposes of the processing, and made available to the required extent (scope and duration) for suitable storage (principle of storage limitation).

Explanation

The purpose represents the control parameter for the data selection and the process steps of the processing. Since a broad definition of the purpose specification hardly develops any controlling effect, it is not sufficient to merely determine the performance of the contract under Art. 6 para.(1) subpara. 1lit. b) GDPR or the fulfilment of legal obligations under Art. 6 (1) subpara.1 lit. c) GDPR as the purpose for data processing. Rather, the precise and specified business purpose and purposes of the processing must be determined for the purpose specification. The other data protection principles can develop their effects only once the purpose has been defined.

Personal data are adequate if they are appropriate from an objective perspective for the respective purpose in terms of function, content, and scope. Personal data are relevant if they make a difference for the fulfilment of the respective purpose, thereby decisively contributing to achieving the respective purpose. Personal data are limited to the necessary extent if the respective purpose of processing cannot be achieved without this data.

Implementation guidance

The principle of transparency is fulfilled if the cloud provider complies with obligations to provide information concerning the data processing (no. 15.1, no. 15.2, and no. 15.3). In addition, transparency, and data minimisation can be achieved by data protection by system design and by default (no. 19.1 and no. 19.2). When processing data for the provision of the service, the cloud provider should make and document considerations and decisions regarding the necessity of the data.

The cloud provider should establish and document TOMs for verifying, rectifying and erasing inaccurate or incomplete personal data for compliance with the principle of accuracy. These include, e.g. test procedures and erasure concepts, designation of a point of contact for cloud users for the receipt of requests, definition of responsibilities and procedural guidelines for prompt processing, and the specification of reporting channels. The TOMs can also be embedded in the existing customer support, troubleshooting or incident management systems.

To comply with storage limitation, the cloud provider should define storage periods for all data or categories of data, which are to be limited to the minimum necessary. In addition, periods should be set for erasing personal data or removing personal references. If data has to be stored due to legal regulations, it should be stored pseudonymously, and the personal reference should only be restored if necessary. Reference is made to the implementation guidance under no. 8.4 on data erasure.

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

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.5.2.1, 6.5.2.2, 7.2.1, 7.2.2 and 7.4.

Reference is made to the implementation guidance in the SDM module 11 “Storing”, module 41 “Plan and specify”, and module 50 “Separation”.

Proof

In principle, a cloud provider can provide insight into TOMs and the data security program as proof of compliance with the data protection principles.

For demonstrating compliance with the principle of transparency, reference is made to the proof contained in the criteria for the obligation to inform about data processing (no. 15.1 and no. 15.3) and to data protection by system design and data protection by default (no. 19.1 and no. 19.2).

To demonstrate compliance with the principles of purpose specification and purpose limitation, a cloud provider should submit a privacy policy as proof that it has determined the purposes for the data processing under its own responsibility and that it has described it clearly and precisely and communicated it to the data subject. In addition, the cloud provider should submit documentation on TOMs, explaining how it processes data logically or physically separately according to the respective processing purposes.

By means of an inspection of the service (e.g. registration of the cloud user) or an asset test (e.g. source code analysis), it can be demonstrated that only the data are processed, which are specified in the documentation and necessary for achieving the purposes. In addition, interviews of employees and the DPO regarding procedural steps and guidelines for data minimisation can be conducted for verification. As a support, a development and design review can demonstrate that the principles of data minimisation, purpose specification and purpose limitation are already taken into account during the application of development or design methods, so that only the data that are necessary for processing are processed and, for example, appropriate data fields in databases are designed to be data-minimising.

A cloud provider submits documents to demonstrate compliance with the principle of data accuracy. This includes, in particular, process documentation for verifying, rectifying and erasing inaccurate or incomplete personal data, as

well as documentation on corresponding (technical) procedures (e.g. settings of database systems). A test rectification or erasure of the data can be carried out as a support. An interview or observation of employees with regard to the verification, rectification and erasure of incorrect or incomplete personal data can be carried out for demonstrating compliance (e.g. regarding the familiarity with the procedural steps and guidelines, clear allocation of responsibilities).

To determine the principle of storage limitation, the cloud provider submits appropriate documents, e.g. erasure concepts (e.g. periods and type of erasure), documentation on pseudonymisation procedures in implementation of the principle of storage limitation or logs on erasures and pseudonymisations. As part of an audit, an interview of employees about storage limitation should be carried out (e.g. regarding knowledge of storage periods, guidelines and procedural steps).

No. 13 – Legal basis for data processing
(Art. 6 (1) subpara. 1 lit. b), c), or f) in conjunction with (2) GDPR)

Criterion

(1) The cloud provider may only process personal data and carry out processing operations that are necessary for the performance of a contract to which the cloud user[59] is a party or for taking steps at the request of the cloud user prior to entering into a contract. In regard to the latter the cloud provider may only process data of the cloud user that will allow it to prepare an offer based on the cloud user´s geographical, technical and individual needs before entering into a legally binding Commissioned Data Processing Agreement. The cloud provider must document structures and procedures leading to the conclusion of a contract or a pre-contractual relationship.

(2) The cloud provider may only process personal data and carry out processing operations that are necessary for compliance with a legal obligation under Member State or EU law to which the controller is subject. The cloud provider must document the legal obligations including the conditions of their occurrence, their scope, and the circumstances of their abolition.

(3) The cloud provider may process personal data and carry out processing operations that are necessary for the purposes of its legitimate interests[60]or those by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the cloud user which require protection of personal data. The cloud provider must document the process of balancing the interests, including the parties involved, whose interests are balanced, the specific interests, fundamental rights and freedoms, and the personal data and processing operations, the balancing criteria having been considered and the result of the balancing, and, if necessary, the compensatory or additional measures to be put in place in order to limit the impact of the processing on data subjects and thus strike a balance between the rights and interests involved.

(4) The cloud provider must verify, determine, and document the legal basis for the processing operations pursuant to (1) to (3).

(5) The cloud provider must have instructions to employees based on which the existence of a sufficient legal basis is to be verified and it defines the corresponding responsibilities for reviews.

Explanation

AUDITOR considers the data processing operations of the cloud provider in its role as controller only to the extent necessary to fulfil the contract with the cloud user on the provision of the cloud service. Since the “cloud user” can also be a natural person, it is also possible, that it is the “data subject” (as indirectly defined by Article 4 no.1 GDPR). The legal basis for data processing is therefore Art. 6 (1) subpara.1 lit. b) GDPR. It permits data processing insofar as it is necessary for the performance of a contract or taking steps prior to entering into a contract with the data subject. The handling of data for the conclusion of a contract, for making changes to the contract, and for the termination of the contract is part of the fulfilment of the contract. Data that are required to enable the use of the cloud service or to invoice the use of the cloud service is also part of the performance of the contract and therefore covered by Art. 6 (1) subpara.1 lit. b) GDPR.

If the cloud provider not only processes data regarding the cloud user for the performance of the contract with the cloud user, but also regarding other data subjects, e.g. the employees of the cloud user, then the cloud provider can invoke Art. 6 (1) subpara. 1 lit. f) GDPR and its legitimate interests, **for as long as the data processing is necessary to perform the contract with the cloud user**, and the interests, fundamental rights and freedoms of

[59] Since the “cloud user” can be a natural person, it is also possible, that it is the “data subject” (as indirectly defined by Article 4 no.1 GDPR).
[60] Since the “cloud user” can be a natural person, it is also possible, that it is the “data subject” (as indirectly defined by Article 4 no.1 GDPR).

the data subject do not override the processing. In this case, the documented balancing of interests must prove that the processing indeed may be based on Art. 6 (1) subpara. 1 lit. f) GDPR.

Where the cloud provider and cloud user conclude a contract on the provision of a cloud service, the cloud provider is obligated to process the cloud user's personal data, among other, based on retention duties under commercial and tax law. Art. 6 (1) subpara.1 lit. c) GDPR permits the data processing for compliance with a legal obligation to which the controller is subject. The actual legal basis for such processing follows from national or European regulations, since Art. 6 (2) GDPR contains an opening clause for the application of such regulations.

Processing operations that are based on the same legal basis can be summarised in their description, review and documentation.

Examples for processing that is necessary to fulfil the contract with the cloud user on the provision of the cloud service are, on the one hand, the fixing of bugs or error analyses, and on the other hand, the fulfilment of service level agreements. In many cases, it is essential to know the context of a process in order to analyse errors. In certain cases, this may also include the processing of personal data. The aim is therefore to clearly diagnose and remedy a possible defect in the service. Likewise, in practice, direct communication with the user may be necessary in some cases. To comply with service level agreements in a specific contractual relationship and to scale resources according to demand, it is necessary to analyse access behaviour and to draw conclusions for resource provisioning. In certain constellations, personal data may also be included in this analysis.

These examples need to be distinguished from cases in which data analyses and possibly profiles are created on the basis of personal data (possibly even about a large number of customers) in order to obtain user preferences 3for the further development of the next generation of the service. Such processing cannot be regarded as necessary to fulfil the contract with the cloud user on the provision of the cloud service.

Implementation guidance

Art. 13 (1) lit. c) or 14 (1) lit. c) GDPR (no. 15.1 or no. 15.2) oblige the cloud provider to inform the data subject of the legal basis of data processing. Therefore, the privacy policy of the cloud provider should not only clearly and precisely determine the purposes of the data processing under its own responsibility, but also specify the concrete legal basis for the data processing.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.15.1, 7.2.1 and 7.2.2.

Reference is made to the implementation guidance in the SDM module 41 "Plan and specify".

Proof

The cloud provider submits the instructions given to employees, by means of which it is reviewed if a sufficient legal basis is given and which states the responsibilities for the reviews.

The cloud provider can submit all of the legally binding agreements or a representative sample of the same, which have been concluded by the cloud provider with the cloud user for the provision of the cloud service. The cloud provider submits an overview of the legal obligations it is subject to for data processing.

The cloud provider submits the documentation of the process of balancing the interests. It can also submit documentation of the balancing of interests that have already taken place. Likewise, as part of an audit, interviews can be carried out with employees regarding the knowledge of the process of balancing the interests.

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

Explanation

It also applies with regard to data processing for the performance of the contract with the cloud user on the provision of the cloud service and for the fulfilment of legal obligations that the cloud provider must ensure by means of TOMs that data are protected in accordance with their need for protection – above all, against security-relevant destruction, loss and unauthorised disclosure.

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

Criterion

(1) The cloud provider must conduct a state-of-the-art risk analysis with regard to data security and must maintain a data security program that corresponds to its protection category and is appropriate for the specific risks of its data processing operations for the provision of the cloud service to the cloud user and

fulfilment of legal obligations, which can result in particular from destruction, loss, alteration, unauthorised disclosure of and unauthorised access to personal data.

(2) The cloud provider must maintain a description of all data and data categories processed by it as a controller for providing the cloud service and fulfilling legal obligations.

(3) In addition to the data security program, the information required in no. 14 can also be given in other documents, provided that as these have been legally bindingly agreed between the cloud provider and cloud user for the commissioned data processing. The requirements for the data security program also apply to these other documents.

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

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

(6) The data security program must be reviewed at regular intervals (at least annually, and after each major change) to ensure that it is up to date and appropriate and it must be updated as necessary.

(7) If the cloud provider involves processors for the performance of the contract with the cloud user, the data security program must describe which data processing operations have been outsourced and are therefore subject to the processor's TOMs.

(8) If the data security program requires security measures of the cloud user, these must be communicated to the cloud user in writing or in an electronic form.

Explanation

Risks of accidental and unlawful destruction, loss, alteration, unauthorised disclosure and unauthorised access to personal data must also be excluded or at least minimised with regard to data processing for the performance of the cloud service and fulfilment of legal obligations. In determining the specific measures, the cloud provider shall not only consider the processing modalities and the probability and severity of the damage, but also the state of the art and the costs for implementation of the measures. The considerations made must be made clear from the data security program.

Implementation guidance

A risk analysis should also be carried out for the data processing operations for the performance of the contract with the cloud user and the fulfilment of legal obligations, which documents the risk assessment approach and methodology. Each risk should be addressed by one or more protective measures. The cloud provider can also use the implementation guidance under no. 2.1 for the creation and maintenance of the data security program regarding the data processing for the performance of the contract with the cloud user and for the fulfilment of legal obligations.

Proof

For demonstrating compliance with the requirements of an appropriate data security program, the explanations under no. 2.1 apply analogously.

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

Criterion

Protection category 1

(1) The cloud provider must protect premises and equipment from damage caused by force majeure[61] and must prevent unauthorised persons from gaining entry to premises and data processing equipment to prevent any knowledge being obtained of the personal data without authorisation and preclude any possibility of manipulating the data processing equipment. The TOMs must generally be appropriate for precluding entry by unauthorised persons due to technical or organisational errors, including operating

[61] Force majeure must be understood as referring to abnormal and unforeseeable circumstances which were outside the control of the party by whom it is pleaded and the consequences of which could not have been avoided in spite of the exercise of all due care. Since the concept of *force majeure* does not have the same scope in the various spheres of application of EU law, its meaning must be determined by reference to the legal context in which it is to operate. C-640/15, ECLI:EU:C:2017:39.

errors of the cloud provider, or due to negligent acts by third parties. At least, the cloud provider must define, document, and implement a set of security requirements for each security zone.

(2) The cloud provider must periodically review (i.e. at least annually or in case of major change) and, if necessary, update the timeliness and adequacy of the authorisations that are required for physical entry to rooms and equipment**.**

(3) Every authorised entry must be logged.

Protection category 2 and 3

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

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

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

Explanation

Reference is made to the explanations in no. 2.2.

Implementation guidance

The implementation guidance under no. 2.2 is applicable.

Proof

The explanations under no. 2.2 apply analogously to the entry protection to premises and equipment.

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

Criterion

Protection category 1

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

(2) The cloud provider must periodically review (i.e. at least annually or in case of major change) the current status and adequacy of rights that are required for admission to data processing systems and update them if necessary.

(3) The cloud provider must protect the admission of authorised persons via the internet by means of a two-factor authentication procedure. Admission via the internet must occur via the use of state-of-the-art transport encryption.

(4) The cloud provider must implement measures for admission control to regularly prevent unauthorised persons from being admitted to data processing systems due to technical or organisational errors, including operating errors of the cloud provider, or due to negligent acts of the cloud user or third parties.

Protection category 2

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

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

Protection category 3

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

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

Explanation

Reference is made to the explanations in no. 2.3.

Implementation guidance

The implementation guidance under no. 2.3 is applicable.

Proof

The explanations under no. 2.3 apply analogously to the proof of admission control.

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

Criterion

Protection category 1

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

(2) The cloud provider must periodically review (i.e. at least annually or in case of major change) the current status and appropriateness of the rights that are required for access to personal data and update them if necessary.

(3) Any access to personal data must be controlled (i.e., monitored and assessed) and logged.

(4) The cloud provider must implement measures to regularly prevent unauthorised persons from accessing personal data due to technical or organisational errors, including operating errors, of the cloud provider or due to negligent acts of the cloud user or third parties.

(5) The cloud provider must protect access by authorised persons via the internet by means of a two-factor authentication.

Protection category 2

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

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

Protection category 3

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

(9) Unauthorised data access must be excluded considering the risk analyses' results. This regularly involves tamper-proof technical measures for the prevention and active detection of attacks. Any unauthorised access and related attempts can be detected afterwards.

Explanation

Reference is made to the explanations in no. 2.4.

Implementation guidance

The implementation guidance under no. 2.4 is applicable.

Proof

The explanations under no. 2.4 apply analogously to the proof of access control.

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

Criterion

Protection category 1

(1) The cloud provider must use state-of-the-art transport encryption for data transmission processes or configure interfaces in such a manner that this is a requirement. The transport encryption used must

ensure that personal data cannot be read without authorisation during electronic transmissions. The encryption keys for an encrypted transmission must be stored securely.

(2) The measures must be appropriate to regularly prevent attacks by unauthorised persons based on technical or organisational errors, including operating errors of the cloud provider or its employees, or negligent acts of the cloud user or third parties. Moreover, the measures must be suitable to prevent any negligent disclosure of data to unauthorised persons by the cloud provider and its employees. Protection must be provided to prevent intentional interference.

(3) The cloud provider must automatically log the metadata of all data transmission operations, including those of recipients and those sent from and to the cloud user or sub-processor. No. 14.6 (1) applies accordingly.

(4) The criteria also apply to the transmissions of data within the cloud provider's own network and that of its processors and between them.

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

Protection category 2

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

(7) The cloud provider must protect the personal data from intentional unauthorised reading, copying, alteration, or deletion and must exclude expectable attempts. The cloud provider must protect against known attack scenarios and normally detects any unauthorised reading, copying, alteration, or deletions (afterwards).

Protection category 3

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

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

Explanation

Reference is made to the explanations in no. 2.5.

Implementation guidance

The implementation guidance under no. 2.5 is applicable, whereas reference is made to no. 7.4.9 instead of no. 8.4.3 of ISO/IEC 27701.

Proof

The cloud provider can demonstrate the protection of data transmissions analogously to no. 2.5.

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

Criterion

Protection category 1

(1) The cloud provider must log entries, alterations, and erasures of data that are required for the performance of the contract for the provision of the cloud service or for the fulfilment of legal obligations to ensure that data processing can be verified and traced afterwards. The cloud provider must observe the principles of necessity, purpose limitation, storage limitation, and data minimization for the logging. The cloud provider must store log data securely.

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

(3) The cloud provider must prevent intentional manipulation by designing the logs of the administrative activities and user activities in such a way that entries, alterations, and erasures can generally be traced even in the event of technical or organisational errors, including operating errors of the cloud provider or its employees or negligent acts by the cloud user or third parties.

Protection category 2

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

(5) The cloud provider must provide protection against expected intentional manipulation of logging instances and against intentional access to or manipulation of logs by unauthorised persons, whereby expectable manipulation attempts are prevented. These protection measures must include in particular adequate protection against known attack scenarios as well as measures by which manipulation can normally be detected (afterwards).

Protection category 3

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

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

Explanation

Reference is made to the explanations in no. 2.6.

Implementation guidance

The implementation guidance under no. 2.6 is applicable. Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.8.

Proof

The cloud provider can prove traceability of the data processing analogously to no. 2.6.

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

Criterion

Protection category 1, 2 and 3

(1) The cloud provider must ensure that login data for the use of the cloud service is stored in encrypted form.

(2) Personal data that must be stored for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations must be stored in encrypted form.

(3) The cloud provider must continuously monitor technical developments relating to encryption. The measures of the cloud provider, particularly secure key management, must comply with the state of the art (as exemplified in the implementation guidance).[62]

(4) Implemented encryption procedures are to be replaced by other encryption procedures when they are no longer compliant with best practice standards.

(5) Unauthorised access to the encryption key must be prevented by means of suitable TOMs.

Explanation

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

Implementation guidance

The implementation guidance under no. 2.9 is applicable.

Proof

The explanations under no. 2.9 apply analogously to the proof of encrypted storage.

No. 14.8 – Separate processing

[62] The state of the art embodies what is currently and generally accepted as best practices, technologies, methodologies, and strategies used to protect information systems. The state of the art does not necessarily imply the most technologically advanced solution but comprises robust technologies and processes, and skilled personnel to defend against evolving data protection threats effectively.

(Art. 5 (1) lit. b) in conjunction with Art. 24, 25, 32 (1) lit. b) and (2) GDPR)

Criterion

Protection category 1

(1) Personal data that is processed for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations must be processed separately by the cloud provider and in accordance with the respective purposes of the processing.

(2) The cloud provider must prevent intentional violations and risks related to data separation in the event of technical or organisational errors, including operating errors, of the cloud provider or its employees.

Protection category 2

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

(4) The cloud provider must exclude expectable intentional violations. This includes protection against known attack scenarios threatening the separation principle. In the context of data storage, the TOMs required to this end must include encryption with individual keys. The cloud provider must normally detect intentional violations of the separation principal (afterwards).

Protection category 3

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

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

Explanation

The criterion promotes the protection goals of availability, integrity, confidentiality, and unlinkability (SDM C1.2 – C1.5), thereby also aiming to secure the principle of purpose limitation under Art. 5 (1) lit. b) GDPR.

Implementation guidance

The implementation guidance under no. 2.10 is applicable. Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.8.

Proof

The cloud provider can prove data separation and its appropriateness analogously to no. 2.10.

No. 15 – Safeguarding the rights of the data subject

Explanation

If the data subject exercises his rights according to Art. 15-22 GDPR by electronic means, the information on actions taken in response to the request should also be provided by electronic means where possible, in accordance with Art. 12 (3) sent. 4 GDPR, unless the data subject has requested another information channel. It should be noted, however, that Art. 20 to 22 GDPR are not considered in Chapter D in the AUDITOR certification.

No. 15.1 – Information to be provided where personal data are collected from the data subject (Art. 13 in conjunction with Art. 12 (1) and Art. 5 (1) lit. a) GDPR)

Criterion

The cloud provider must ensure by means of TOMs that it informs the data subjects at the time of the collection of its personal data for the performance of the contract on the provision of the cloud service and for the fulfilment of legal obligations about the circumstances of the processing and their rights as data subjects in an intelligible form using clear and plain language. The cloud provider must inform the data subject of all information required under Art. 13 (1) and (2) GDPR.

Explanation

Pursuant to Art. 13 GDPR, the cloud provider is obligated to inform the data subjects of the circumstances of the direct data collection. This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Implementation guidance

The cloud provider should provide the cloud user with its privacy policy containing all information under Art. 13 (1) and (2) GDPR when registering for the use of the cloud service (e.g. via the website or the information portal of the cloud service). The cloud provider should provide a point of contact for the cloud user with appropriate availability and authorisations, who can initiate the immediate fulfilment of the rights of the data subject.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.1, 7.3 and 7.5.

Reference is made to the implementation guidance in the SDM module 41 “Plan and specify”.

Proof

The cloud provider submits its template privacy policy containing the information pursuant to Art. 13 (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 demonstrate that the cloud provider has provided all information in accordance with Art. 13 (1) and (2) GDPR. To fulfil its obligation to inform other data subjects such as, e.g. the employees of the cloud user, the cloud provider can also submit a template of its privacy policy, which it transmits to the employee, e.g. via email, when the data are collected.

No. 15.2 – Information to be provided where personal data have not been obtained from the data subject (Art. 14 in conjunction with Art. 12 (1) and Art. 5 (1) lit. a) GPPR)

Criterion

> If personal data have not been obtained directly from the data subject for the performance of the contract on the provision of the cloud service and for the fulfilment of legal obligations (third-party collection), the cloud provider must ensure by means of TOMs that the data subject is informed, within an appropriate period and in an intelligible form, using clear and plain language, about the circumstances of the processing and the rights of the data subjects, unless the provision of such information is impossible or would involve a disproportionate effort. The information to the data subject must include all information required pursuant to Art. 14 (1) and 2 GDPR.

Explanation

This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C.2.7).

Implementation guidance

The cloud provider should ensure the allocation of responsibilities and reporting channels, and document these to be able to inform the data subject in a timely manner. The appropriateness of the period for providing information is based on the specific circumstances of the processing. According to Art. 14 (3) lit a) GDPR, the period is at the latest one month after obtaining the personal data. Shorter periods apply if the personal data are to be used for communication with the data subject or be disclosed to other recipients. In the first case, Art. 14 (3) lit. b) GDPR, the cloud provider must comply with its obligation to provide information at the latest at the time of the first communication to that data subject. In the second case, the information can be provided according to Art. 14 (3) lit. c) GDPR at the latest when the personal data are first disclosed to the recipient.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.1, 7.3 and 7.5.

Proof

The cloud provider should submit its template privacy policy, containing the information pursuant to Art. 14 (1) and (2) GDPR, which it makes available to the data subject. In addition, it should submit documentation on the reporting procedure, e.g. procedural steps, reporting channels or logs of completed reports.

No. 15.3 – Access to information (Art. 15 in conjunction with Art. 5 (1) lit. a), 3rd alt. GDPR)

Criterion

> The cloud provider must ensure by means of TOMs that it grants the data subject access to the personal data upon request that it processes as the controller for the performance of the contract on the provision of the cloud service and for the fulfilment of legal obligations. The cloud provider must provide a copy of this data to the data subject.

Explanation

This criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Implementation guidance

Pursuant to Art. 12 (3) GDPR, the cloud provider is to provide the data subject access to his data without undue delay and in all cases within one month of receipt of the request. The request process should be as simple as possible, which is why contact forms or customer self-services should be provided via an online platform. Pursuant to Art. 15 (3) GDPR, the data subject has the right to receive a copy of the personal data undergoing processing.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.3.1, 7.3.2, 7.3.3, 7.3.6, 7.3.8 and 7.3.9.

Proof

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to provide information promptly to the data subjects (e.g. mechanisms and reporting channels, service descriptions). Whether the information was actually provided can also be verified by means of process documentation.

As part of an inspection, an access to data can be carried out on a test basis to demonstrate that access and data can be provided (e.g. by means of a technical function within the cloud service or by manual inquiries to the cloud service support).

No. 15.4 – Rectification and completion (Art. 16 in conjunction with Art. 5 (1) lit. d) GDPR)

Criterion

The cloud provider must ensure by means of TOMs that it grants data subjects the possibility to correct or erase any incomplete or inaccurate personal data relating to the provision of the cloud service on their own. Alternatively, the cloud provider must perform the (legitimate) rectification or erasure.

Explanation

The cloud provider is obligated under Art. 16 GDPR to rectify inaccurate personal data and to complete incomplete personal data of data subjects upon request. The rectification pursuant to Art. 16 GDPR promotes the protection goal of intervenability (SDM C1.7).

Implementation guidance

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

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.3.1, 7.3.2, 7.3.6 and 7.3.9.

Reference is made to the implementation guidance in SDM module 61 "Correction".

Proof

The cloud provider can demonstrate compliance with the requirements by documenting which measures it has taken to enable the (direct) rectification and completion of data or the rectification and completion of data subjects by themselves (e.g. documentation of the relevant mechanisms and reporting channels, service descriptions). Whether the data were actually rectified and completed can also be verified by means of process documentation.

As part of an inspection, representative test rectifications and completions can be carried out. This can be done, for example, by means of a technical function within the cloud service or by manual inquiries to the cloud service support.

No. 15.5 – Erasure (Art. 17 (1) GDPR)

Criterion

(1) The cloud provider must ensure by means of TOMs that it erases personal data processed by it for the performance of the contract on the provision of the cloud service upon request by the data subject and on its own initiative without undue delay when the requirements of Art. 17 (1) lit. a), d) or e) GDPR are met. The erasure must be unrecoverable, so that no information about the data subject can be obtained from it. The cloud provider ensures that erasure is irrevocably by using state of the art measures.

(2) The cloud provider must ensure that the personal data processed by it for the performance of the contract on the provision of the cloud service is not only erased from the active data base, but also from copies and data backups.

(3) The cloud provider must ensure that the erasure will be repeated for the relevant data after data are recovered, which have already been erased from the active data base but not from the data backup yet.

Explanation

The criterion promotes the protection goals of intervenability and unlinkability (SDM C1.7 and C1.5). In particular, there is no obligation to erasure if the cloud provider is obligated to process the data for compliance with a legal obligation (Art. 17 (3) lit. b) GDPR).

Since Art. 17 GDPR is based on an unrecoverable erasure, measures of logical erasure such as the removal of personal data from directories by erasure commands are not sufficient to meet the requirements of Art. 17 GDPR.

It is referred to the implementation guidance under ISO / IEC 27701 no. 7.3.1, 7.3.6, 7.3.9 and 7.4.7.

Implementation guidance

To be able to comply with its erasure obligations, the cloud provider should create an erasure concept by means of which it can continuously determine and check its erasure obligations. The erasure concept should include criteria that can be used to determine whether a data record must be erased or stored due to retention periods. Metadata such as the purpose of the processing, the definition of indicators for the loss of statutory permissions, retention periods, and the legal basis for the storage should therefore be laid down for each data record.

Since the erasure of data in backup and fail-safe systems is more time-consuming than erasure from the active database, copies and data from backup systems can also be erased at later points in time from active database, e.g. in the course of overwriting or destroying the affected data media. As a rule, the erasure in the backup files should take place no later than one year after erasure in the active database, whereas it should be aimed for shorter periods.

The implementation guidance under no. 6.4 is applicable.

Proof

The cloud provider can prove its 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.

The possibilities for demonstrating compliance under no. 6.4 are applicable.

No. 15.6 – Restriction of processing
(Art. 18 (1) and (3) GDPR)

Criterion

(1) The cloud provider must ensure by means of TOMs, that, upon the data subject's request, it can restrict the processing of personal data processed by it for the performance of the contract with the cloud user on the provision of the cloud service or for the fulfilment of a legal obligation.

(2) The cloud provider must ensure by means of TOMs that it informs the data subject before the restriction of processing is lifted.

Explanation

Pursuant to Art. 18 (1) GDPR, the cloud provider is obligated to restrict the processing of personal data under certain conditions, so that the data cannot be further processed or modified. The criterion promotes the protection goal of intervenability (SDM C1.7).

Implementation guidance

A restriction of processing can be implemented, for example, by a temporary transmission to another processing system or by blocking.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.3.1, 7.3.2, 7.3.3 and 7.3.9.

Reference is made to the implementation guidance in the SDM module 62 "Restrict processing".

Proof

The cloud provider can demonstrate compliance with the requirements by documenting the measures it has taken to restrict the processing of data and to inform the data subject before the restriction is lifted. It can submit logs of requests made by data subjects and the subsequent restrictions.

In the course of an inspection, restrictions (including notification to the data subject) and the lifting of these can be carried out on a test basis. The restriction can be simulated, for example, by a technical function within the cloud service or by manual inquiries to the cloud service support. As part of an audit, interviews (e.g. to gain knowledge of procedural steps, etc.) and observations can be used to demonstrate the way in which restrictions are implemented and how they are lifted again, and how the data subject is notified.

No. 15.7 – Notification obligation in the event of rectification, erasure or restriction of processing (Art. 19 in conjunction with Art. 5 (1) lit. a) 3rd alt. GDPR)

Criterion

Insofar as the cloud provider has disclosed to recipients data subject's personal data processed by it for the performance of the contract with the cloud user on the provision of the cloud service or due to legal obligations, it must ensures by means of TOMs that it communicates every rectification or erasure of personal data and every restriction of processing to each recipient and informs the data subject about the recipients if the data subject so requests.

Explanation

The cloud provider is obligated under Art. 19 GDPR to notify recipients – to whom it has disclosed personal data – of any rectification, erasure, or restriction of processing and to inform the data subject of the recipients upon request. The criterion promotes the protection goals of transparency and intervenability (SDM C1.6 and C1.7).

Recipients are, for example, processors that are engaged for the performance of the contract on the provision of the cloud service.

Reference is made to the implementation guidance of ISO/IEC 27701 no. 7.3.1, 7.3.2, 7.3.3, 7.3.7 and 7.3.9.

Proof

The cloud provider can prove its compliance with the requirements by documenting the measures it has taken to meet its notification obligation and its duty to inform the data subject on request about the recipient of the disclosure (e.g. documentation of the relevant mechanisms and reporting channels, service descriptions). A cloud provider can submit logs of notifications that have been issued.

In the course of an inspection, a test notification can be carried out (e.g. by a technical function within the cloud service or by manual inquiries to the cloud service support). As part of an audit, interviews (e.g. to gain knowledge of procedural steps, etc.) and observations can also be used to demonstrate whether a notification can be carried out. Likewise, it can be checked whether a cloud user can be informed of the recipients of the disclosure on request.

No. 15.8 – General information obligation, information obligation in the event of inaction or delayed request processing (Art. 12 (3) and (4), Art. 15 to 19 GDPR)

Criterion

(1) The cloud provider must ensure by means of TOMs that it informs the data subject on actions taken on request under Art. 15 to 19 GDPR as relates to the data processing performed by it as the controller for the performance of the contract on the provision of the cloud service and for fulfilment legal obligations, without undue delay, whereas at the latest within one month after receipt of the request.

(2) The cloud provider must ensure by means of TOMs that it informs the data subject if it does not answer his request in accordance with Articles 15 to 19 GDPR as relates to the data processing performed by it as the controller for the performance of the contract on the provision of the cloud service and for fulfilment legal obligations, without undue delay, whereas at the latest within one month. The information refers to the extension of the period and the reasons for this.

(3) The cloud provider must ensure by means of TOMs that it informs the data subject, at the latest within one month, if it does not take action to answer its request in accordance with Art. 15 to 19 GDPR as relates to the data processing performed by it as the controller for the performance of the contract on the provision of the cloud service and for fulfilment legal obligations. The information of the data subject must refer to the reasons for inaction and the possibility to lodge a complaint with the supervisory authority or to seek a judicial remedy.

Explanation

According to Art. 12 (3) sent. 1 GDPR, the cloud provider has to provide the data subject with the necessary information on actions taken on a request under Art. 15 to 22 GDPR without undue delay, whereas at the latest

within one month after receipt of the request. Art. 20 to 22 GDPR are not considered in Chapter D in the AUDITOR certification. The cloud provider, therefore, has to respond to the requested action on each request from a data subject pursuant to Art. 15 to 19 GDPR. If the cloud provider relies on a (national) exception to the rights of the data subject when answering requests, it must therefore adequately explain the reasons to the data subject for rejecting his request in part or in full.

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

Art. 12 (4) GDPR obligates the cloud provider to inform the data subject, at the latest within one month, of the reasons why it does not, despite a request pursuant to Art. 15 to 19 GDPR, take action to comply with the request. Reasons not to comply with a request are, e.g. unfounded or excessive requests according to Art. 12 (5) sent. 2 lit. b) GDPR. Furthermore, according to Art. 12 (4) GDPR, the data subject must be informed of his option to lodge a complaint with the supervisory authority pursuant to Art. 77 GDPR or to seek a judicial remedy pursuant to 79 GDPR.

Implementation guidance

The cloud provider should express, as concisely, intelligibly and clearly as possible, which actions it has taken to comply or not to comply with the request of the data subject. Especially if the request of a data subject has been partially or completely rejected, the reasons for this should be described as detailed as possible, so that the data subject can assess whether it would like to take actions against the cloud provider (e.g. a complaint to the supervisory authority).

It should also be expressed, as concisely, intelligibly and clearly as possible, why a longer period is required for processing the request and this period should be specified. The same applies to naming the reasons for inaction.

Proof

Process documentation and logs can be used to prove if information has in fact been provided and to the complete extent to the data subject.

No. 16 – Notification of personal data breaches (Art. 33 (1), (3) to (5) GDPR)

Criterion

(1) The cloud provider must have a process in place for notifying personal data breaches arising from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, including the definition of procedural steps, deadlines and measures for the identification, analysis, and evaluation of the personal data breach and its reporting, the responsibilities, and the awareness-raising of the employees involved.

(2) The cloud provider must notify the supervisory authority without undue delay as soon as it becomes aware of personal data breaches[63] arising from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, if the personal data breach is likely to result in a risk to the rights and freedoms of the cloud user.

(3) When assessing the risks to the rights and freedoms of the cloud user, the cloud provider must take into account the type of breach; the nature, sensitivity, and volume of personal data; the ease of identification of individuals; the severity of consequences for individuals; the special characteristics of the cloud user; its own special characteristics as the cloud provider and the number of affected individuals.

(4) The cloud provider must maintain a process and measures to identify, analyse, and evaluate the risk to the rights and freedoms of the data subjects.

(5) The cloud provider must document any personal data breaches, including the facts relating to the personal data breach, its effects, and the remedial actions taken.

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

[63] Where feasible, not later than not later than 72 hours after having become aware of it.

(7) The cloud provider must determine which factors must be fulfilled so that for making an assumption that a risk to the rights and freedoms of the cloud user can be expected and the person who is responsible for the notification. The competent employees must be sufficiently trained to be able to assess violations.

Explanation

The cloud provider is obligated to notify personal data breaches to the supervisory authority under Art. 33 GDPR without undue delay insofar as they are likely to result in a risk to the rights and freedoms of natural persons. The cloud provider must document personal data breaches in a manner enabling the supervisory authority to verify the cloud provider's compliance with the requirements of this Article. The criterion promotes the protection goal of integrity and transparency (SDM C1.3 and C1.6).

The personal data breach is to be considered "likely to result in a risk to the rights and freedoms of the cloud user", when the risk-assessment concludes with the result, that both, i.e. the likelihood and the severity of the risk to the rights and freedoms of the data subject, are given. Since the data breach has already occurred, i.e. is not of a hypothetical nature, the focus of the assessment is wholly about the resulting risk of the impact of the breach on individuals. The cloud provider should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring as should be regarded as mandatory by "Guidelines 9/2002 or personal data breach notification under GDPR" (Version 2.0, adopted 28 March 2023). The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which is useful when designing the breach management response plan (ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity).

Implementation guidance

The cloud provider should document its risk assessment whether a personal data breach is to be considered "likely to result in a risk to the rights and freedoms of the cloud user", including the condition assessed in accordance with (3) and the assessment results.

The cloud provider should establish and document corresponding processes, as well as define contact persons, responsibilities and reporting channels. The notification of personal data breaches should be integrated in the incident and troubleshooting management of the cloud provider to enable processing in a timely manner.

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

Reference is made to the implementation guidance in ISO/IEC 27701 no. 6.13.1.

Official reporting forms can be used to notify personal data breaches to the supervisory authority.

Proof

The cloud provider can demonstrate compliance with the requirements by documenting in its data security program the way in which it notifies of personal data breaches. The cloud provider can also submit further documentation, including, for example, process documentation for notification, directories of procedures and instructions, guidelines, templates for notifying of personal data breaches, decision-making rules for assessing personal data breaches, procedures for risk assessment and factors that can be included in the risk analysis, as well as reporting channels and responsibilities. Documented notifications of personal data breaches can also be submitted if existing.

Prove can also be provided by interviewing employees or observation of a test notification. As part of an on-site audit, it should be demonstrated that sufficient resources are available to ensure notifications without undue delay.

A cloud provider should also submit documents for training the responsible employees (e.g. certificates, confirmations of participation in workshops) and allow that they participate in interviews as part of an audit (e.g. with regard to the awareness of guidelines and procedural steps).

No. 17 – Communication of a personal data breach to the data subject (Art. 34 (1) to (3) GDPR)

Criterion

(1) The cloud provider must communicate personal data breaches to the data subject without undue delay, which arise from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject.

(2) The communication must contain at least the information under Art. 33 (3) lit. b), c) and d) GDPR in clear and plain language.

(3) The cloud provider must maintain a procedure for the identification, analysis, and evaluation of personal data breaches arising from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, based on which it is determined which factors must be fulfilled so that a high risk to the rights and freedoms of the data subject can be assumed, which deadlines are to be observed, and the person who is responsible for the communication. The competent employees must be sufficiently trained to be able to assess violations.

(4) The communication according to (1) and (2) may be omitted if the requirements of Art. 34 (3) GDPR are met.

(5) The cloud provider must document the communications of data subjects about personal data breaches arising from the processing of data for the performance of the contract on the provision of the cloud service or for the fulfilment of legal obligations, and of the circumstances, reasons, and measures when the communication to data subjects in accordance with (4) does not take place.

Explanation

A high threat level, which requires communication to the data subject in accordance with Art. 34 GDPR, can be assumed, for example, in the event that bank and credit card information are lost. Such data are often processed for the purpose of performing the contract with the cloud user, whereby the obligation to communicate personal data breaches may become relevant.

The communication to the data subject referred to in Art. 34 (1) GDPR is not required in accordance with Art. 34 (3) GDPR if one of the following conditions is met:

a. the controller has implemented appropriate technical and organisational protection measures, and these measures were applied to the personal data affected by the personal data breach, in particular such measures that render the personal data unintelligible to any person who is not authorised to access it, e.g. by encryption;

b. the controller has taken subsequent measures, which ensure that the high risk to the rights and freedoms of data subjects referred to in (1) is no longer likely to materialise;

c. the communication would involve disproportionate effort. In such a case, there a public communication or similar measure is to be implemented, whereby the data subjects are informed in an equally effective manner.

Implementation guidance

The implementation guidance under no. 8.2 is applicable, whereas reference is made to no. 7.3.1 and 7.3.2 instead of no. 8.2.5 and 8.3 of ISO/IEC 27701.

Proof

The cloud provider can submit the data security program and the TOMs described therein for communicating personal data breaches and other documentation as evidence, including, e.g. the process documentation with the procedural steps and deadlines for communicating personal data breaches to data subjects, guidelines, templates for communicating to the data subjects, decision-making rules for assessing personal data breaches, procedures for the risk analysis and the factors that are included to the risk analysis, including the reporting channels and responsibilities. In addition, employee interviews can be conducted as part of an audit to demonstrate that the specified procedure for notifying data subjects is known and implemented in the company.

If available, the cloud provider can also submit communications to data subjects regarding personal data breaches that have been issued in the past already.

The communication to the data subject about the personal data breach may be omitted only on the conditions of Art. 34 (3) GDPR. In this regard, the cloud provider should in particular submit documentation, e.g. in the data security program, which defines the TOMs that it has taken to ensure that there are no longer any high risks to the rights and freedoms of the data subject in the future. The documentation should also show which risks are addressed by the measures. The TOMs can also be subjected to an inspection. If the data subjects have not received individual communication, documentation of the public announcement can be submitted, e.g. in a daily newspaper and an explanation that the effort involved was disproportionate.

No. 18 – Maintaining a record of processing activities (Art. 30 (1), (3) to (5) GDPR)

Criterion

(1) If the cloud provider is obligated to maintain records of processing activities, this record must refer to the processing activities that it carries out for the performance of the contract on the provision of the cloud service legal obligations. The record must also contain the content listed in Art. 30 (1) lit. a) to g) GDPR.

(2) The cloud provider must maintain a process for updating the record of processing activities if processing activities are introduced or eliminated, or if the information according to Art. 30 (1) lit. a) to g) GDPR changes for the listed processing activities.

(3) For the purpose of updating the record of processing activities, the cloud provider must maintain processes for cooperation between the specialist operational departments involved in the processing activities, its representative and, if applicable, the DPO and must regulate the internal responsibilities for this.

(4) The record of processing activities must be maintained in writing, including in electronic form and the storage locations must be known.

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

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

Explanation

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

As a rule, cloud providers with more than 250 employees are obligated to maintain records of processing activities. However, cloud providers with fewer employees who process data to provide the cloud service to the cloud user generally also have to maintain records of processing activities, since this processing takes place regularly and not only occasionally, so that the exception under Art. 30 (5) GDPR is not applicable.

According to Art. 30 (2) GDPR, the representative of the cloud provider, if one is designated, must also maintain a record of processing activities.

Implementation guidance

The implementation guidance under no. 8.3 is applicable.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 7.2.8.

Proof

The cloud provider can prove that records of processing activities have been maintained analogously to no. 8.3.

No. 19 – Data protection by design and by default

No. 19.1 – Data protection by system design (Art. 25 (1) in conjunction with Art. 5 (1) and (2) GDPR)

Criterion

Within the framework of the service design, the cloud provider must conduct a risk analysis and ensure by means of TOMs that only personal data necessary for the performance of the contract on the cloud service processed in the cloud service and that the remaining principles of Art. 5 GDPR are implemented in the cloud service.

Explanation

While the cloud provider, in its role as the processor, is only an indirect addressee of Art. 25 GDPR, the cloud provider as the controller is a direct addressee. The cloud service technology and organisation must be designed in such a way that they support the data protection principles of Art. 5 GDPR in the best possible way. The cloud provider must ensure that it only processes personal data that are necessary for the provision of the service to the cloud user when designing the service. The extent of the processing of the data and the storage period must be limited to what is necessary to achieve the purpose of processing.

Implementation guidance

The implementation guidance under no. 9.1 is applicable, whereas reference is made to no. 7.4 instead of no. 8.4 of ISO/IEC 27701.

Proof

For demonstrating compliance with data protection by system design, the explanation in no. 9.1 applies analogously.

No. 19.2 – Data protection by default
(Art. 25 (2) in conjunction with Art. 5 (1) and (2) GDPR)

Criterion

(1) The cloud provider must ensure by default setting that only personal data that are necessary for providing the cloud service are processed for the initial start-up and use of the cloud service in regard to the amount of personal data collected, the extent of their processing, and the period of their storage and the access to personal data is also limited to what is necessary[64].

(2) The cloud provider must ensure by default that personal data are not made accessible without the individual's intervention to an indefinite number of natural persons and that no inappropriate risks[65] arise for the data subject from providing in a too expansive extent[66] access to personal data available.

Implementation guidance

The implementation guidance under no. 9.2 is applicable. Instead of the no. 8.4 of ISO/IEC 27701 referred to in no. 9.2, no. 7.4 is applicable.

Proof

For demonstrating compliance with data protection by default, the explanation in no. 9.2 applies analogously.

[64] In regard to the latter the cloud provider must ensure that persons acting under its authority shall access the personal data only on a need to know basis.
[65] Inappropriate risks arise from not taking 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 natural persons posed by the processing.
[66] A "too expansive extent" is given if a technical or personal access grants more information as is necessary for the relevant purpose of the processing.

No. 20 – Order processing by the cloud provider

Explanation

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

No. 20.1– Services governed by a legally binding agreement (Art. 28 (3) subpara. 1 sent. 2 GDPR)

Criterion

(1) Where the cloud provider outsources the processing of data necessary for the performance of the contract on the cloud service to a processor, it must conclude a legally binding Commissioned Data Processing Agreement with the processor.

(2) The cloud provider must ensure by means of appropriate TOMs that data are not processed until after a legally binding Commissioned Data Processing Agreement has been concluded with the processor.

(3) The legally binding Commissioned Data Processing Agreement must be drafted in writing or an electronic form.

(4) The legally binding Commissioned Data Processing Agreement g must meet the following requirements of this criterion, whereas the required definitions can may also be made in other documents if these have been included into the legally binding Commissioned Data Processing Agreement.

(5) The cloud provider must ensure that the object and duration of the processing are outlined as specifically as possible in the legally binding Commissioned Data Processing Agreement.

(6) The cloud provider must ensure that the legally binding Commissioned Data Processing Agreement determines the nature and purpose of the intended processing, the nature of data processed, and the categories of data subjects.

(7) The cloud provider must ensure that the legally binding Commissioned Data Processing Agreement determines that personal data will only be processed by the processor in accordance with documented instructions by the cloud provider, even as relates to the transfer of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor must inform the cloud provider of the legal requirement obligation before the processing, unless that law prohibits such information on important grounds of public interest. In this case, the legally binding Commissioned Data Processing Agreement contains the obligation of the processor to notify the cloud provider of these legal requirements before processing, unless that law in question prohibits such information on important grounds of public interest.

(8) In case the commissioned data processing includes the instruction-bound transfer of personal data to third countries or international organisations, the cloud provider must ensure that the legally binding Commissioned Data Processing Agreement determines the instruments according to Art. 45 GDPR or Art. 46 (2) and (3) GDPR, which are to be used for the transfers and, if applicable, also the other supplementary measures to be taken to ensure an appropriate level of protection.

(9) The cloud provider must ensure that the legally binding Commissioned Data Processing Agreement determines that the processor undertakes to inform the cloud provider if it believes that an instruction from the cloud provider infringes data protection regulations.

(10) The cloud provider must ensure that the legally binding Commissioned Data Processing Agreement determines the place of the data processing. If the data processing takes place outside the EU or the EEA, the specific third country must be stated.

(11) The cloud provider must ensure that the processor undertakes in the legally binding Commissioned Data Processing Agreement to notify the cloud provider without undue delay of any changes of the place of the data processing.

(12) The cloud provider must ensure that the legally binding Commissioned Data Processing Agreement determines that, before the start of the data processing operations, the processor commits the persons authorised to process personal data to confidentiality that continues to apply beyond the end of their employment relationship, unless they are already subject to a suitably comparable statutory obligation of confidentiality.

(13) The cloud provider must ensure that, in accordance with Art. 32 GDPR, the TOMs appropriate to the level of security of the outsourced data processing are determined in the legally binding Commissioned Data Processing Agreement.

(14) The cloud provider must ensure that the legally binding Commissioned Data Processing Agreement determines how the processor complies with the requirements in accordance with Art. 28 (2) and (4) GDPR for the use of the services of other processors.

(15) The obligations of the processor to return data media, return data and for unrecoverable erase data after the end of the data processing must be set out in the legally binding Commissioned Data Processing Agreement.

(16) The legally binding Commissioned Data Processing Agreement must include information on support for the cloud provider in fulfilling the rights of the data subject and in its notification obligation in the event of data breaches.

Explanation

Since the cloud provider is seeking certification of its data processing operations, it must ensure that data processing by a sub-processor also complies with the requirements of the General Data Protection Regulation. For this, the cloud provider must first conclude a legally binding Commissioned Data Processing Agreement with the processor that includes the obligation requirements under Art. 28 (3) subpara. 1 sent. 2.

Implementation guidance

The implementation guidance under no. 1 apply analogously to the conclusion of a legally binding agreement with a sub-processor.

Reference is made to the implementation guidance in ISO/IEC 27701 no. 5.4.1.2, 5.4.1.3, 6.10.2.4, 6.12, 7.2.6.

Proof

The cloud provider submits the legally binding Commissioned Data Processing Agreement (s) containing the corresponding stipulations, which it has concluded with the order processor(s). Documents such as the data security program including TOMs or certificates should be proven for the respective subcontractors. Other relevant documents can be included as proof such as the template contract for commissioned data processing with sub-processors, guidelines and instructions, further guarantees from the sub-processors, internal control areas of the cloud provider by means of sub-processor audits, the data protection concept or the risk assessment for subcontracting.

No. 20.2 – Ensuring proper processing

Criterion

(1) The cloud provider must ensure that the processor processes personal data exclusively on the cloud provider's documented instructions (Art. 28 (3) subpara. 1 sent. 2 lit. a) and h), Art. 29; 32 (4) GDPR).

(2) The cloud provider must ensure that the processor informs the cloud provider if, in its opinion, an instruction infringes data protection regulations (Art. 28 (3) subpara. 1 sent. 2 lit. h) in conjunction with Art. 29 GDPR).

(3) The cloud provider must ensure for outsourced processing that the processor guarantees the confidentiality, integrity, and availability of data and systems, the resilience of the systems, and the availability of and access to data after a physical or technical incident. The processor must regularly (at least annually, and after each major change) check and, if necessary, adapt the implemented TOMs (Art. 24, 25, 28, 32, 35 in conjunction with Art. 5 (1) lit. f) and (2) GDPR).

(4) The cloud provider must ensure that the processor obligates its employees to commit themselves to confidentiality remaining valid beyond the end of their employment relationship before data processing begins, unless they are subject to a statutory obligation of confidentiality (Art. 28 (3) subpara. 1 sent. 2 lit. b) and h) GDPR).

(5) The cloud provider must ensure that the processor entrusts only employees, who have the necessary professional knowledge and who are trained in data protection and data security with the performance of processing operations (Art. 28 (3) subpara. 1 sent. 2 lit. e) and f) GDPR)

(6) The cloud provider must ensure that the processor informs the cloud provider if the place of the data processing changes (Art. 28 (3) subpara. 1 sent. 2 lit. a) and h) GDPR).

(7) The cloud provider must ensure that the processor deletes or returns all the data media provided to it and all personal data after the end of the performance of services relating to processing or upon instruction

from the cloud provider, and that it unrecoverably deletes existing copies (Art. 28 (3) subpara. 1 sent. 2 lit. g) and h) GDPR).

(8) The cloud provider must ensure that the processor assists the cloud provider for the fulfilment of the rights of the data subjects and documents all instructions for exercising the data subject's rights (Art. 28 (3) subpara. 1 sent. 2 lit. e) and h) in conjunction with Chapter III GDPR).

(9) The cloud provider must ensure that the processor designates a DPO if it is legally obligated to do so (Art. 37 to 39 GDPR, Sec. 38 (1); (2) in conjunction with Sec. 6 (5) sent. 2 BDSG).

(10) The cloud provider must obligate the processor to maintain a record of processing activities if it is legally obligated to do so (Art. 30 (2) to (5) GDPR).

(11) The cloud provider must ensure that the processor notifies the cloud provider without undue delay after becoming aware of a personal data breach and its extent (Art. 33 (2) and Art. 28 (3) subpara. 1 sent. 2 lit. f) GDPR).

(12) The cloud provider must ensure that the processor complies with all requirements under the legally binding Commissioned Data Processing Agreement pursuant to No. 20.1 and fulfils all requirements under these criteria (Art. 24 (1) GDPR).

(13) The cloud provider must ensure that the processor ensures, if it also uses sub-processors, that the further sub-processors comply with the requirements set out in the criteria no. 10.1 to 10.5 in Chapter V.

(14) If the commissioned data processing provides for the instruction-bound transfer of personal data to third countries or international organisations or if the processor is subject to the law of a third country, which obligates it to disclose personal data to public authorities of the third country, although the data processing exclusively takes place in the EU or in the EEA, the cloud provider must ensure that the processor complies with criterion no. 11.1 from Chapter VI (Art. 46 in conjunction with Art. 42 (1) and 2; Art. 48 GDPR).

(15) The cloud provider must obligate the processor to appoint a representative in accordance with criterion no. 11.2 under Chapter VI if the processor is legally obligated to do so (Art. 27 in conjunction with Art. 3 (2) GDPR).

Explanation

If the cloud provider engages a processor for processing data to fulfil the contract for the provision of the cloud service, it must not only conclude a legally binding Commissioned Data Processing Agreement to this effect, which fulfils the requirements under Art. 28 (3) subpara. 1 sent. 2 GDPR, but it must also ensure that the processor implements the measures set out in the legally binding Commissioned Data Processing Agreement and fulfils its other obligations under the General Data Protection Regulation.

Implementation guidance

Reference is made to the implementation guidance in ISO/IEC 27701 no. 5.4.1.2, 5.4.1.3, 6.12, 7.2.6

Proof

The cloud provider can prove its compliance with the requirements by submitting documentation, test results or similar evidence from the processor that has convinced it of the assumption that the processor complies with all of the obligations that apply to it under the General Data Protection Regulation and therefore has the sufficient guarantees according to Art. 28 (1) GDPR at his disposal. These can be codes of conduct that are followed, certificates, legally binding Commissioned Data Processing Agreement s (in particular, with regard to instructions from the cloud provider and obligations of the sub-processor), service descriptions, data security programs or other documents. In addition, the cloud provider can submit documents on the selection (e.g. records on selection considerations and decisions) and the implementation of its own controls (e.g. records of the subcontractor controls).

As further support, an interview of the employees can be conducted in the course of an audit regarding the implementation of the control of sub-processors (e.g. as to familiarity with procedural steps and guarantees of the sub-processors). Employees can also be interviewed on the involvement of sub-processors in the support functions and duties as main processors (e.g. regarding familiarity with procedural steps and contact persons for the sub-processors).

No. 21 – Data transfers: Appropriate safeguards for data transfers; measures for protection against disclosure of data to public authorities of third countries

(Art. 45, 46 and Art. 48 GDPR) [67]

Pre-Explanation

It may be possible, that the cloud provider - in its role as the controller – transfers data of the cloud user or persons working for it in the framework of its business/enterprise. This might be due to e.g. technical, legal or other reasons. For example, a technical update/support from abroad of its server-supplier in ongoing business operations might lead to the situation, where a cloud user is using the cloud service, although the systems are currently being worked on by the technical support. Another example could be that a cloud provider, as the controller of its systems and their processing is legally required to do so by EU- or member state law. Therefore, corresponding criteria are to be put in place that safeguard that transfers in that respect are also governed by GDPR´s regime. In this regard it is the controller for its business solution, processing personal data. It transfers data under its own responsibility and, where applicable, under its own legal obligation

Criterion

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

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

(3) If, after assessing law and practice of the third country, the appropriate safeguards within the meaning of Art. 46 (2) or (3) GDPR prove to be insufficient for ensuring an adequate level of protection equivalent to that of the General Data Protection Regulation, the cloud provider must take supplementary measures[68] to ensure this adequate level of data protection. Otherwise, the data transfer must not take place.

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

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

Explanation

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

It should be noted that the regulation of Art. 49 GDPR does not contain any permissions for the systematic and regular data transfer between exporter and importer[69], as it is customary in cloud computing. Systematic and regular data transfers between exporter and importer must therefore be based on adequacy decisions pursuant to Art. 45 (3) GDPR or the appropriate safeguards pursuant to Art. 46 (2) or (3) GDPR. Data transfers on the basis of Art. 49

[67] Transfer refers to the movement of personal data when it is transferred from the EU/EEA to a country or countries outside the EU/EEA.

[68] E.g. TOMs in accordance with EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of personal data.

[69] Data exporter is/are the natural or legal person(s), public authority/ies, agency/ies or other body/ies (“entity/ies”) transferring the personal data. The entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity is/are the data importer. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

GDPR may take place, if at all, only in very restrictive exceptional cases which, however, are not covered by this Criteria Catalogue.

Further reference is made to the explanation in no. 11.1.

Implementation guidance

Reference is made to the implementation guidance in 11.1.

Proof

Reference is made to the proof section in no. 11.1.

E. References

BSI C5	Cloud Computing Compliance Controls Catalogue, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html, status 2020
BSI TR-02102-1	Cryptographic Mechanisms: Recommendations and Key Lengths, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html, status 22.02.2019
BSI TR-02102-2	Cryptographic Mechanisms: Recommendations and Key Lengths. Part 2 – Use of Transport Layer Security (TLS), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html, status 22.02.2019
BSI TR-02102-3	Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.html, status 25.01.2018
BSI TR-02102-4	Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Secure Shell (SSH), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.html, status 25.01.2018
DIN EN 1627	Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification, status 2011
DIN 66398	Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information, status 2016
DIN 66399	Destruction of data carriers, status 2012
EU Cloud CoC	EU Cloud Code of Conduct, EU Data Protection Code of Conduct for Cloud Service Providers, status December 2020, https://eucoc.cloud
Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679	European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf
Guidelines 4/2019 on Article 25 Data Protection by Design and by Default	European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, version 2.0, adopted on 20 October 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
Guidelines 07/2020 on the concepts of controller and processor in the GDPR	European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.1, adopted on 20 September 2022, https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf
Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR	European Data Protection Board, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, version 2.0, adopted 14.02.2023, https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf
Guidelines 9/2022 on personal data breach notification under GDPR	European Data Protection Board, Guidelines 9/2022 on personal data breach notification under GDPR, version 2.0, adopted 28.03.2023, https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf
ISO/IEC 11770-2	IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques, status 2018

ISO/IEC 19941	Information technology — Cloud computing — Interoperability and portability, status 2017
ISO/IEC 21964-1	Information technology — Destruction of data carriers — Part 1: Principles and definitions, status 2018
ISO/IEC 24760-1	IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts, status 2019
ISO/IEC 24760-2	Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements, status 2015
ISO/IEC 24760-3	Information technology — Security techniques — A framework for identity management — Part 3: Practice, status 2016
ISO 25237	Health informatics — Pseudonymization, as of 2017
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls, status 2013
ISO/IEC 27018	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, status 2019
ISO/IEC 27040	Information technology — Security techniques — Storage security, status 2015
ISO/IEC 27701	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, status 2019
ISO/IEC 29101	Information technology — Security techniques — Privacy architecture framework, as of 2018
ISO/IEC 29134	Information technology — Security techniques — Guidelines for privacy impact assessment, as of 2017
ISO/IEC 29146	Information technology — Security techniques — A framework for access management, as of 2016
ISO 31000	Risk management – Guidelines, status 2018
IEC 31010	Risk management — Risk assessment techniques, status 2019
SDM	Standard-Datenschutzmodell (Standard Data Protection Model), Version 3.0, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V3.pdf, status 2022
SDM module 11 “Storage”	Baustein 11 „Aufbewahren“, Version: V1.0, status 6.10.2020, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
SDM module 41 “Plan and Specify”	Baustein 41 „Planen und Spezifizieren, Version: V1.0, status 25.03.2021 https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
SDM module 42 “Documentation”	Baustein 42 „Dokumentieren“, Version: V1.0a, status 2.09.2020, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
SDM module 43 “Logging”	Baustein 43 „Protokollieren“, Version: V1.0a, status 2.09.2020 https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
SDM module 50 “Separation”	Baustein 50 „Trennen“, Version: V1.0, status 06.10.2020, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
SDM module 51 “Control access to data, systems and processes”	Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, Version: V1.0, status 01.11.2021, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
SDM module 60 “Erase and destroy”	Baustein 60 „Löschen und Vernichten”, Version: V1.0a, status 2.09.2020, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
SDM module 61 “Correction”	Baustein 61 „Berichtigen“, Version: V1.0, status 06.10.2020, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
SDM module 62 “Restrict processing”	Baustein 62 „Einschränken der Verarbeitung“, Version: V1.0, status 6.10.2020, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell
Simitis/Hornung/ Spiecker gen. Döhmann, Datenschutz-recht	Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht. DSGVO mit BDSG. NOMOS Kommentar. https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FSimHorSpiKoDatenSchR_1%2Fcont%2FSimHorSpiKoDatenSchR%2Ehtm
Working paper „Requirements for the use of pseudonymisation solutions in compliance with data protection regulations”	Schwartmann/Weiß (ed.), Requirements for the use of pseudonymisation solutions in compliance with data protection regulations, a working paper of the Data Protection Focus Group of the Platform Security, Protection and Trust for Society and Business at the Digital Summit 2018, https://www.gdd.de/downloads/requirements-for-the-use-of-pseudonymisation-solutions

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data	European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021, https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
Recommendations 02/2020 on the European Essential Guarantees for surveillance measures	European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.