Federal Ministry
for Economic Affairs
and Energy

Criteria catalogue for cloud services

Version 2.0

Version 2.0
31. Mai 2018
Trusted Cloud

Document history

Version	Date	Author	Comments
1.0	01.02.2016	Trusted Cloud	Document released
1.1	18.08.2016	Trusted Cloud	Document released
2.0	31.05.2018	Trusted Cloud	Document released

Table of contents

1 Introduction

The Trusted Cloud criteria catalogue for cloud services defines the minimum requirements which a cloud service must fulfill for obtaining the Trusted Cloud label and thus must fulfill in order to be listed on the Trusted Cloud Portal.

The version 2.0 of the Trusted Cloud criteria catalog for cloud services has been adapted to the extended requirements of the European General Data Protection Regulation (GDPR). The GDPR has to be fulfilled when processing personal data since May 25th 2018.

The document is structured as below. Chapter 2 describes the basic concepts and requirements on which the criteria catalogue is based respectively were incorporated into its development. The structure of the criteria catalogue is explained in chapter 3. Chapter 4 describes in detail the criteria and minimum requirements of the criteria catalogue which have to be met for listing a cloud service on the Trusted Cloud Portal.

2 Basic concepts

The basic concepts and requirements, which have been incorporated in the development of the criteria catalogue, are described in this section.

2.1 Requirements for the criteria catalogue

The following requirements were considered for the development of the criteria catalogue.

2.1.1 General requirements

- The criteria catalogue contains a minimum amount of criteria and criteria measures in order to evaluate a cloud service in the required depth for the Trusted Cloud label.
- Thus, the criteria must cover all areas relevant for the cloud users: contractual aspects, quality of service provisioning, data privacy, data security.
- The criteria catalogue defines minimum requirements which a service must fulfill in order to be listed on the Trusted Cloud Platform.
- The criteria must be suitable to request and to analyze it in the context of self-tests from the provider.
- The criteria catalogue must be versioned.

The requirements of the criteria catalogue can also be differentiated according to the stakeholders of the Trusted Cloud Portal which are described in the following sections.

2.1.2 Requirements of cloud users

- The Trusted Cloud criteria catalogue is transparent to the user.
- The criteria are suitable for the selection and comparison of reliable cloud services i.e. they make a statement regarding
    - Data security
    - Data privacy
    - Legal conformity
    - Integration of the services into existing infrastructure
    - Avoidance of additional dependencies
    - Security of investment

The criteria are suitable for the selection of cloud services processing personal data.

2.1.3 Requirements for cloud provider

- The criteria and characteristics must be understood i.e. it must be transparent, why a criterion is requested.
- The criteria can be specified in context of a self-test at a reasonable cost.
- The minimum requirements for the listing of a service must be clearly visible and already communicated transparently before registration.

2.2 Alignment and testing scope

The focus of the available version of the Trusted Cloud criteria catalogue is on criteria which increase the provider transparency, especially on the representation of all subcontractors engaged in service provisions such as data center, contract design and ensuring data sovereignty by the user.

Furthermore, the criteria and controls safeguarding data security are integral components of this catalogue.

The criteria with regard to data protection aim to demonstrate the appropriate implementation of the requirements of the European General Data Protection Regulation (GDPR). This may also be confirmed by providing corresponding certificates.

Another essential objective of the Trusted Cloud criteria catalogue is the description of a cloud service from a user view by specifying criteria of transparency. In addition to the functional description of the services the catalogue thus contains criteria for representing the technical and functional pre-requisites for use, migration and exchange of the service as well as information about the required processes for the provision of services and ensuring service level agreements like availability and support services.

The Trusted Cloud criteria catalogue was designed such that it is filled out in a legally-binding self-assessment by the cloud service provider. The provider can verify individual information by mentioning certificates and seal of approvals. The test takes place by the Trusted Cloud bearer organization by plausibility check of the provider information. Currently no additional audit of the provider is performed.

2.3 Types of data processing

The version 2.0 of the Trusted Cloud criteria catalogue introduces a differentiation between possible intended purposes of a cloud service in processing data. Different types of data to be processed may constitute varying requirements with regard to data security, data privacy and contract design.

The type of data processing is specified by the provider. Possible characteristics are:

- Data processing activities (i.e. the service requested from the cloud service) that do not contain, produce, or sustain information or protection-meriting information
- Personally Identifiable Information (PII)

By selecting the suitability of a cloud service for the processing of PII the service has to fulfill different criteria and minimum requirements for obtaining the Trusted Cloud label.

2.4 Minimum requirements

Minimum requirements differentiate between requirements that serve the transparent representation of the cloud service and requirements that require a minimum characteristic of a specific quality criterion of the service or the service provision.

One can find additional details in section 3.2 on the different minimum requirements of the criteria catalogue.

2.5 Further development and versioning

The Trusted Cloud criteria catalogue is continuously updated and further developed by the Trusted Cloud bearer organization. This can include both adding of new criteria, change of existing criteria as well as an adjustment of the minimum requirements.

By modifying the criteria catalogue, a new version of the criteria catalogue is set. The updated version of the criteria catalogue is mandatory for the listing of new services and the renewal of the listing of existing services respectively. An early renewal of the listing within the validity period and based on the updated version of the criteria through incentives of the providers is conceivable, for example by corresponding perquisite of the listing fees.

2.6 Used sources

The following sources were evaluated and included for the conception of the Trusted Cloud criteria catalogue for cloud services:

Table 1: Evaluated sources

Source	Description
ESCA Training Material - Part D Catalogue [1]	Eurocloud Star Audit-criteria catalogue for the certification
Requirement catalogue Certified Cloud Service [2]	Criteria catalogue TÜV Rheinland for the certification „Certified Cloud Service“
ISO / IEC 27001 [3]	ISO / IEC Standard 27001 for information security management systems
ISO / IEC 27002 [4]	ISO / IEC Standard 27002 for control mechanisms for the information security
ISO / IEC 27018 [5]	ISO / IEC Standard 27018 for processing of personal data in Cloud
Cloud-Service-Certification [6]	Framework and criteria catalogue for certification of cloud services.
CSA Cloud Controls Matrix [7]	Framework for secure cloud services of Cloud Security Alliance
Trust in Cloud Check list [8]	Criteria catalogue for certification “Trust in Cloud”
Cloud Industry Forum Code of Practice [9]	Criteria catalogue of Cloud Industry Forums for secure cloud services
Security recommendations for Cloud Computing provider [10]	Key issues paper for implementation of measures for secure cloud computing from provider’s view
Selection table for assignment of security-technical requirements [11]	Table for individual assignment of technical requirements in a suitable and reliable cloud service
Requirement catalogue for Cloud-provider (draft) [12]	BSI requirement catalogue for cloud provider for ensuring confidentiality, availability and integrity.
The CIS critical security controls for effective cyber defense [13]	Control mechanisms for security against cyber-attacks
The standardization and standardized environment of Cloud Computing [14]	Inquiry from European and German view of inclusion of technology program „Trusted Cloud“
Manual for formation of contracts for Cloud Computing [15]	Trusted Cloud-manual for formation of contracts
Intel Cloud finder [16]	Market place for searching for cloud services
EU GDPR [17]	European General Data Protection Regulation (GDPR).

3 Structure of the criteria catalogue

The trusted cloud criteria catalogue for cloud services consists of several areas which contain a sequence of criteria. Each criterion is sub-divided into one or more characteristics which must be specified by the provider in order to describe a cloud service.

3.1 Areas and criteria

The Trusted Cloud criteria catalogue is structured into the following areas:

Table 2: Areas of criteria catalogue

Area	Objective
A.1 Provider	Representation of providers, the ownership structure and the capability for provision of cloud services
A.2 Service	Functional description of the service
A.3 Subcontractor and data centers	Information about related subcontractors or data centers for service-provision
A.4 Certificates	Representation of certificates of the provider or subcontractor
A.5 Contract	Representation of relevant contractual components for the secure cloud usage
A.6 Security	Representation of technical and organizational measures for ensuring data and IT security
A.7 Data privacy	Representation of technical and organizational measures for ensuring data privacy and other legal determining factors
A.8 Operative processes	Representation of required processes for the provision of services and ensuring SLA
A.9 Interoperability & portability	Representation of technical and functional prerequisites for use, migration and change of services
A.10 Architecture	Description of underlying technical architecture of the service

Each area is subdivided into several criteria which are shown in below table:

Table 3: Overview of criteria

ID	Criterion	Target
A1. Provider		
A.1.1	Legal contract provider and ownership structure	The legal form of provider and governing associate is known
A.1.2	Company profile	Representation of capacity and experience of the provider for provision of cloud services
A.1.3	Auditability	Whether and in which scope audits of the provider by the user are possible
A.2 Service		
A.2.1	General information about the service	Specification of basic information for descriptions of the service
A.2.2	Functional description of the service	Clarification of functional requirements in reference to company demand
A.2.3	Maturity level of the service	Information about the extent of the service usage
A.2.4	References	Information about reference customers and use cases
A.2.5	Main contact to the service	Information about the main contact to the service
A.2.6	Other contacts to the service	Information about other contacts related to the service
A.2.7	Type of data processing	Information about the type of data processing
A.3 Subcontractors and data centers		
A.3.1	Subcontractors or owners and location of data centers	Clarification of location of data and related subcontractors
A.3.2	Company profile	Information about size of the company, number of employees, main business fields
A.4 Certificates		
A.4.1	Seal of approval / certificate of provider of the service or the service in itself	Information about seal of approval and certifications of the provider or the service
A.4.2	Seal of approval / certificate for subcontractors or data centers	Information about certification of data centers and the technical infrastructure
A.5 Contract		
A.5.1	General transparency of contract	Contracts are completely available beforehand and changes in the active contract are due to obtain consent

ID	Criterion	Target
A.5.2	Rights of use and area of jurisdiction	Information about usability rights and area of jurisdiction
A.5.3	Transparency of subcontractors	Naming of all related subcontractors on the service provision and agreements in the case of change during duration as well as their commitment for data privacy requirements
A.5.4	Rules for service interruption or insolvency	Clear rules are provided which guarantee adequate restitution of data at any time
A.5.5	Service Level Agreements	Information about contractual rules of Service Level Agreements
A.5.6	Transparent price model	Traceable and transparent billing of services
A.5.7	Change Management	Information about contractual rules for Change Management
A.5.8	Obligation to co-operate and provision of customers	Concrete determination of obligation to cooperate, provisions and additional tasks of cloud customers
A.5.9	Copyright and rights of use	Grant author and patent rights for rights of use and indemnification of possible third party requirements
A.5.10	Exit support/Support at contract termination	Rules for exit support (Exit-Management)
A.6 Security		
A.6.1	Security management	Proof of efficient management of information security by suitable certifications
A.6.2	Management of security incidents	Information about the process in case of security incidents and about emergency situation management
A.6.3	Security certificates	Information about certificate of evidence of implemented measures for IT security (for example EuroCloud, TÜV, CSA Star, IT-basic security, ISO 27001 etc.)
A.6.4	Certification of data centers and the technical infrastructure	Information about certificate of data centers and the technical infrastructure
A.6.5	Encryption	Information about used encryption techniques for encrypting data transmission and storage
A.6.6	Identity- and accessmanagement	Information about the rights and roles concept

ID	Criterion	Target
A.7 Data privacy		
A.7.1	Technical and organizational measures	Representation of implementation of technical and organizational measures for data security
A.7.2	Formal data privacy requirements	Adherence to national data privacy requirements
A.7.3	Demonstration of compliance	Information on confirmation of compliance with the obligations laid down in the GDPR
A.7.4	Location of data retention	Limitation of the hosting of customer data on specified regions
A.7.5	Implementation of data subject rights	Information about the implementation of the data subject rights
A.7.6	Employees data security obligations and awareness	Details on employee commitment to data secrecy
A.7.7	Data privacy certification	Information about available data privacy certificate
A.8 Operative processes		
A.8.1	Service management	Proof of efficient service management for ensuring service quality
A.8.2	Service management certificate	Information about certificate for proof of service quality
A.8.3	Service availability	Information about assured service availability in SLA
A.8.4	Backups	Information on backup options and implementation of data protection concepts
A.8.5	Provisioning	Description of possibilities for provisioning of service by the user
A.8.6	Support	Information about support-services
A.9 Interoperability & portability		
A.9.1	Technical standards	Representation of technical standards of set Service Stacks
A.9.2	Data export	Representation of procedures for data access on customer data and for data restitution
A.9.3	Integration	Description of procedures for technical integration of services in existing IT-landscape

ID	Criterion	Target
A.9.4	Technical and organizational prerequisites for use of service	Description of technical and organizational prerequisites for use of service
A.10 Architecture		
A.10.1	Isolation	Representation of measures for delimiting client areas for dedicated technical infrastructures and data areas
A.10.2	Scaling	Representation of possibilities for scalability of the technical infrastructure

Each criterion contains a sequence of characteristics which must be specified by the service provider. Characteristics are described by means of the following attributes:

ID	Characteristic	Feature	Minimum requirement	Remark

<ID>:

ID of the characteristic

<Characteristic>:

Description of the characteristic

<Feature>:

Feature of the characteristic. The following types are distinguished:

- **Free text:**
  The characteristic is to be specified by the service provider filling in any text.
- **Binary selection:**
  The characteristic is either met or not met. (For example information yes/no).
- **Selection lists:**
  The characteristic is to be specified by selection of an answer from a list of defined reply possibilities.

<Minimum requirement>:

Minimum requirement which must be met by a service for listing on Trusted Cloud Portal (also see section 3.2).

<Remark>:

Further detailing of the characteristic, for example completion instructions or information on the testing process of the characteristic.

The detailed description of the characteristics is in section 4.

3.2 Minimum requirements

The criteria catalogue defines the following types of minimum requirements:

- **Mandatory information**

  Characteristics which are featured as mandatory information must be specified immediately by the proposer. In addition, no qualitative valuation of the information takes place.

  Example:

Characteristic	Attribute	Minimum requirement
Company name	Free text	Mandatory information

- **Qualitative minimum requirement**

  Characteristics which are specified as free text can be featured with a qualitative minimum requirement.

  Example:

Characteristic	Attribute	Minimum requirement
Information about used price model	Free text	Transparent representation of the price model including costs for booking additional cloud capacities.

- **Concrete minimum requirement**

  Characteristics that own concrete attributes can be featured as minimum requirement with a concrete attribute.

  Example:

Characteristic	Attribute	Minimum requirement

Are all concerned subcontractors specified on service provision?	• No information • All concerned sub-contractors can be named on request • All concerned sub-contractors are specified	All concerned subcontractors can be named on request

3.3 Information about certificates and seal of approval

Appropriate seals of approval and certificates can be specified for proof of individual criteria such as security and data privacy features of cloud services. The following general characteristics are to be specified for each seal of approval and certificate which may be considered (see A.4 for details):

Table 4: Characteristics certificate

ID	Characteristic
A.4.1.1	Name of the certificate
A.4.1.2	Type of the certificate
A.4.1.3	Description of the scope of testing
A.4.1.4	Certification authority
A.4.1.5	Document of the certificate
A.4.1.6	Validity date
A.4.1.7	Is the certificate regularly audited?

The proof takes place by transmission of corresponding documents to the Trusted Cloud test organization.

In addition to this general information, an additional description for individual criteria can be mentioned in terms of relevance of the certificate for the concrete area (see for example area A.6 Security).

Table 5: Additional information on the relevance of certificate

ID	Characteristic	Attribute
A.6.2.1	Name of the certificate	List of mentioned certificates in A.4
A.6.2.2	Further details of certificate in	Free text

	terms of test scope, attributes, extensions etc.	

4 Criteria for cloud services

In this section the criteria for listing cloud services on Trusted Cloud Portal are described in detail. An explanation of the structure of the criteria catalogue is in section 3.

A.1 Provider

Transparent representation of the provider, the enterprise profile and information on auditability by the user.

A.1.1 Legal contract provider and ownership structure

The criteria contain information about the identity of the provider like address and register number or sales tax-ID/VAT-ID, information as well as contact addresses of main contact person.

The proof takes place via the supplied excerpt from the commercial or cooperative register or a comparable official registry or directory.

Target: The legal form of the provider and governing partner is known.

Table 6: Legal contract provider and ownership structure

ID	Characteristic	Attribute	Minimum requirement	Remark
A.1.1.0	Type of application	Cloud service, Cloud consultants & cloud service	Mandatory information	

ID	Characteristic	Attribute	Minimum requirement	Remark
A.1.1.1	Name of the company	Free text	Mandatory information	
A.1.1.2	Legal form	Free text	Mandatory information	
A.1.1.3	Sales tax-ID/VAT-ID	Free text	Mandatory information either A.1.1.3 or A.1.1.4	
A.1.1.4	Register number	Free text	Mandatory information either A.1.1.3 or A.1.1.4	
A.1.1.5	Date of registration	Date	Mandatory information	
A.1.1.6	Does your company belong to the category of "small and medium-sized enterprises" (SMEs) according to EU Recommendation 2003/361/EC?	Yes, no	Mandatory information	
A.1.1.7	Address of the head office or main subsidiary	Free text	Mandatory information	Street, house number, location, country
A.1.1.8	Names of the members of the substitute organization or the legal representatives	Free text	Mandatory information	
A.1.1.9	Main contact	Free text	Mandatory information	Name, telephone number, email address
A.1.1.10	Contact data protection officer acc. Art. 37 para. 5 GDPR or alternative Data privacy contact	Free text	Mandatory information	At least one data privacy contact has to be specified. Choice whether qualification for data protection officer is met. Name, telephone number, email address

ID	Characteristic	Attribute	Minimum requirement	Remark
A.1.1.11	Contact IT department	Free text		Name, telephone number, email address
A.1.1.12	Contact of legal department	Free text		Name, telephone number, email address
A.1.1.13	URL of the company website	Free text	Mandatory information	
A.1.1.14	Description of the company	Free text		
A.1.1.15	Logo of the company	File format png, gif or jpg		More information: The file has to be smaller as 2 mb. Allowed file formats are png, gif, jpg, jpeg.

A.1.2 Company profile

The company profile includes characteristics for representing the size of the company as well as information on the experience of provision of cloud services.

Target: Representation of the performance and experience of the provider in the provision of cloud services.

Table 7: Profile of the enterprise

ID	Characteristic	Attribute	Minimum requirement	Remark
A.1.2.1	Number of employees	Free text	Mandatory information	
A.1.2.2	Number of employees in area of	Free text	Mandatory information	

ID	Characteristic	Attribute	Minimum requirement	Remark
	cloud services			
A.1.2.3	Sales	Free text	Mandatory information	
A.1.2.4	Category of the company	Reseller, ISV, CSP, others	Mandatory information	
A.1.2.5	Number of public offered cloud services	Free text	Mandatory information	
A.1.2.6	Experience grade of provision of cloud services	No information, < 1 year, 1-5 years, > 5 years	Mandatory information	

A.1.3 Auditability

Description of the possibilities of performing audits by the user.

Target: Specify whether and to what extent is audit possible by the user.

Table 8: Auditability

ID	Characteristic	Attribute	Minimum requirement	Remark
A.1.3.1	Is it possible for the customer to ask/ apply for an external audit?	Yes, no	Mandatory information	
A.1.3.2	If yes, which audits were already performed?	Free text	Mandatory information	
A.1.3.3	Can audits on processes and organizational procedures related to data protection and security be conducted?	No information, By the user, By a third person (mandated auditor)	Mandatory information	

A.2 Service

Functional description of the services.

A.2.1 General information about the service

Specification of basic information for describing services.

Target: Basic classification of the service as per provision type and service-model.

Table 9: General information about the service

ID	Characteristic	Attribute	Minimum requirement	Remark
A.2.1.1	Name of the service	Free text	Mandatory information	
A.2.1.2	Logo of the service	PDF or JPG file		The logo of the service will be presented in the overview of the cloud services listed. Please choose a graphic, which is at least 400 x 200 px large. If there does not exist a logo of your service than please use your company logo as an alternative.
A.2.1.3	Provision-type	Public/Private/Hybrid	Mandatory information	
A.2.1.4	Service-model	IaaS PaaS SaaS	Mandatory information	
A.2.1.5	URL of the service website	Free text	Mandatory information	

A.2.2 Functional description of the service

Functional description of the service and functional categorization of the service.

Target: Clarification of functional requirements in reference to enterprise demand.

Table 10: Functional description of the service

ID	Characteristic	Attribute	Minimum requirement	Remark
A.2.2.1	Service description	Free text	Mandatory information	
A.2.2.2	Brief description of the service	Free text	Mandatory information	Functional brief description of the service as part of the overview of the cloud services presented on the Trusted Cloud Portal.

A.2.3 Maturity level of the service

Details on the scope of service usage.

Target: Representation of maturity level of the service.

Table 11: Maturity level of the service

ID	Characteristic	Attribute	Minimum requirement	Remark
A.2.3.1	Number of customers who use the service including date of enquiry	Free text		
A.2.3.2	Number of overall users who use the service including date of enquiry	Free text		

A.2.4 References

Information on reference customers and use cases.

Several reference customers can be mentioned. All listed characteristics are to be specified for each reference customer.

Target: References can be mentioned by name and the productive use is documented comprehensibly.

Table 12: References

ID	Characteristic	Attribute	Minimum requirement	Remark
A.2.4.1	Name of the customer	Free text		
A.2.4.2	Description of use	Free text		
A.2.4.3	Contact person	Free text		Name, telephone number, email address
A.2.4.4	URL of the website of the customer	Free text		

A.2.5 Main contact to the service

Information on the main contact to the service.

Table 13: Main contact to the service

ID	Characteristic	Attribute	Minimum requirement	Remark
A.2.5.1	Name	Free text		
A.2.5.2	Position	Free text		
A.2.5.3	Telephone number	Free text		
A.2.5.4	Email address	Free text		
A.2.5.5	Image	Browse, upload		More information: The file has to be smaller as 2 mb.

				Allowed file formats are png, gif, jpg, jpeg.
A.2.5.6	Address	Country, address 1, address 2, postcode, city		

A.2.6 Other contacts to the service

Information about other contacts related to the service.

Table 14: More contacts to the service

ID	Characteristic	Attribute	Minimum requirement	Remark
A.2.6.1	Name	Free text		
A.2.6.2	Position	Free text		
A.2.6.3	Telephone number	Free text		
A.2.6.4	Email address	Free text		
A.2.6.5	Image	Browse, upload		More information: The file has to be smaller as 2 mb. Allowed file formats are png, gif, jpg, jpeg.

A.2.7 Type of data processing

Information about the type of data processed by the service.

Table 15: Type of data processing

ID	Characteristic	Attribute	Minimum requirement	Remark

A.2.7.1	What kind of data may be processed?	no information;
		personal data acc. to the GDPR;		

A.3 Subcontractors and data centers

The information is to specify for each data center or any subcontractor that are directly linked with the service provision or indirectly can gain access to data areas of the services.

A.3.1 Subcontractors or owners and location of the data centers

Clarification of data location and related subcontractors.

Target: The location of data retention (incl. backup and failover) is named correctly.

Table 16: Subcontractors or owners and location of the data centers

ID	Characteristic	Attribute	Minimum requirement	Remark
A.3.1.1	Name of the company	Free text	Mandatory information	
A.3.1.2	Legal form	Free text	Mandatory information	
A.3.1.3	Register number	Free text		
A.3.1.4	Address of head office or main subsidiary	Free text	Mandatory information	Street, house number, location, country – question is important whether another legal order facilitates access to data by governing partner (e.g. from USA)
A.3.1.5	Geographical location of data center	Free text	Mandatory information	Country, state the exact location of the data center should not be requested (security risk) but the Geo location (if required up to level of state).
A.3.1.6	Part of the company / legally independent company	Part of the company, legally independent company	Mandatory information	Information whether the data center is a part of the applicant company or a legally independent company
A.3.1.7	Logo of the subcontractor / data center	File format png, gif or jpg	Mandatory information	More information: The file has to be smaller as 2 mb. Allowed file formats are png, gif, jpg, jpeg.
A.3.1.8	URL of the website of the subcontractor or data center	Free text	Mandatory information	

A.3.2 Company profile

Information about size of the company, number of employees, main business fields.

Target: Representation of performance ability and experience of the provider for provision of cloud services.

Table 17: Company profile

ID	Characteristic	Attribute	Minimum requirement	Remark
A.3.2.1	Number of employees	Free text		These fields are mandatory fields for white-label-products of the provider.
A.3.2.2	Sales	Free text		
A.3.2.3	Category of the company	Reseller, ISV, CSP, others	Mandatory information	
A.3.2.4	Number of publicly offered cloud services	Free text		
A.3.2.5	Experience grade of provision of cloud services	No information, < 1 year, 1-5 years, > 5 years		

A.4 Certificates

Information about seals of approval and certificates of the cloud service and on the service provision of concerned subcontractors or data centers.

A.4.1 Seal of approval/ certificate of service

Information about seals of approval and certificates of the services.

For each service, multiple certificates can be registered. If a certificate is specified, then all listed characteristics of the certificate are to be mentioned. Proof takes place via transferred documents.

Target: Proof of information on implemented measures in the area of IT-security, data security, service management etc.

Table 18: Seal of approval/ certificate of the service

ID	Characteristic	Attribute	Minimum requirement	Remark
A.4.1.1	Name of the certificate	List of relevant certificates, free text for other certificates	Mandatory information	

A.4.1.2	Type of the certificate	BSI IT-Grundschutz;
		CSA Star;
		EuroCloud Star Audit;
		EuroPrise;
		FedRAMP;
			Mandatory information	

ID	Characteristic	Attribute	Minimum requirement	Remark

		ISAE 3402/SSAE 16 Typ II;
		ISO 27001;
		ISO 27018;
		Trust in Cloud;
		Trusted Cloud – TÜV;
		TRUSTed Cloud Privacy Zertifizierung;
		TÜV Cloud Security;
		TCDP;
		others		

A.4.1.3	Description of the scope of test	Free text	Mandatory information	Details about scope and representation of relevance for the offered service
A.4.1.4	Certification authority	Free text	Mandatory information	Name of the company, address
A.4.1.5	Document of the certificate	PDF or JPG file	Mandatory information	
A.4.1.6	Validity date & valid thru	Date	Mandatory information	
A.4.1.7	Is the certificate regularly audited?	Yes/ no	Mandatory information	

A.4.2 Seal of approval/ certificate of the subcontractors or data centers

Details about certifications of data centers and the technical infrastructure.

Multiple certificates can be registered. If a certificate is specified, then all listed characteristics of the certificate are to be mentioned. Proof takes place via transferred documents.

Target: Proof of information on implemented measures in the area of IT security, data privacy, service management, etc., of the subcontractors involved in provision of the service or the data centers.

Table 19: Seal of approval/ certificate of the subcontractors or data centers

ID	Characteristic	Attribute	Minimum requirement	Remark
A.4.2.1	Name of the certificate	List of relevant certificates, free text for other certificates	Mandatory information	

A.4.2.2	Type of the certificate	BSI IT-Grundschutz;
		CSA Star;
		EuroCloud Star Audit;
		EuroPrise;
		FedRAMP;
		ISAE 3402/SSAE 16 Typ II;
		ISO 27001;
		ISO 27018;
			Mandatory information	

ID	Characteristic	Attribute	Minimum requirement	Remark

		Trust in Cloud;
		Trusted Cloud – TÜV;
		TRUSTed Cloud Privacy Zertifizierung;
		TÜV Cloud Security;
		TCDP;
		others		

A.4.2.3	Description of the scope of test	Free text	Mandatory information	Details about scope and representation of relevance for the offered service
A.4.2.4	Certification authority	Free text	Mandatory information	Name of the company, address
A.4.2.5	Document of the certificate	PDF or JPG file	Mandatory information	
A.4.2.6	Validity date & valid thru	Date	Mandatory information	
A.4.2.7	Is the certificate regularly audited?	Yes/ no	Mandatory information	

A.5 Contract

Representation of the relevant contract components for secured cloud use.

A.5.1 General transparency of contract

Information about general contract transparency.

Target: Contracts are completely available for users beforehand and are in reference.

Table20: General transparency of contract

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.1.1	Are contracts available beforehand to the customers?	No information, Total contract documents can be viewed by the user on demand and are in reference (General terms and conditions, service contract, SLA, data privacy agreement), Total contract documents are visible on the website of the provider publicly as well as available to the user and is in reference (General terms and conditions-service contract -SLA-data privacy agreement)	Total contract documents for the user are visible on demand and in reference (General terms and conditions, service contract, SLA, data privacy).	Terms of Service, Service Level Agreements, data privacy clarification, Web-URL of the contract documents
A.5.1.2	Web reference for service	Free text	Mandatory information	

ID	Characteristic	Attribute	Minimum requirement	Remark
	contract			
A.5.1.3	Details of used licenses	Free text		transparent representation of required/ used licenses

A.5.2 Rights of use and area of jurisdiction

Details about rights of use and area of jurisdiction. For a listing, EU contract law is mandatory.

Target: Information on the concrete location of the area of jurisdiction.

Table 21: Rights of use and area of jurisdiction

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.2.1	Rights of use	No information, German contract law EU contract law	EU contract law	Selection "EU Contract Law" concrete contract law must also be specified in a free text field
A.5.2.2	Area of jurisdiction	City		Since applicable law must be EU contract law, the area of jurisdiction must be within the EU, so here query the specific place acc. Contract details

A.5.3 Transparency with subcontractors

Name all concerned subcontractors and agreements for change during duration of service provision as well as commitment on data privacy information.

Target: Transparency in direct related partner on service provision.

Table22: Transparency with subcontractors

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.3.1	Are all concerned subcontractors specified in service provision?	No information, All concerned subcontractors can be named as per demand, All concerned subcontractors are specified	All concerned subcontractors can be named as per demand	The immediate concerned partner (e.g. data center) and partner are to be understood as subcontractor for service provision, due to its function an immediate access is maintained for the managed data areas (server, hard discs, archiving).
A.5.3.2	Are all contract conditions (SLA, data privacy information) transferable to subcontractors are adhered by these contractually?	No information, All subcontractors obligate for adherence of contract conditions, Adherence of contract conditions by the subcontractor is explicitly structured	All subcontractors obligate for adherence of contract conditions	

ID	Characteristic	Attribute	Minimum requirement	Remark
		contractually		

A.5.4 Rules for service interruption or insolvency

Clear rules are provided which guarantee data feedback at any time.

Target: Ensuring data sovereignty of the user.

Table 23: Rules for service interruption or insolvency

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.4.1	Is access to customer data as well as security of customer data in case of insolvency of the provider or a special ending of the contract ensured or contractually structured?	No information, Rules for data feedback are not part of the contract. Clear rules are provided which guarantee adequate data feedback in case of insolvency or special ending of contract or interruption of service provision.	Clear rules are provided which guarantee adequate data feedback in case of insolvency or special ending of contract or interruption of service provision.	
A.5.4.2	Details about contractually ensured rules for feedback of	Free text	Mandatory information	

ID	Characteristic	Attribute	Minimum requirement	Remark
	customer data			

A.5.5 Service Level Agreements

Information of Service Level Agreements (SLA) and rules for SLA-violations.

Target: SLAs are component of the contract and there are rules for SLA-violations.

Table 24: Service Level Agreements

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.5.1	Are service-level-agreements component of the contract?	Yes/ no	Mandatory information	
A.5.5.2	Is it possible to review the compliance with the SLA by the customer?	Yes/ no	Mandatory information	
A.5.5.3	Description of SLAs and testing procedures	Free text		
A.5.5.4	Are the legal consequences for breach against the SLAs described in the contract?	Yes/ no	Mandatory information	
A.5.5.5	Is there lasting contractual guarantee to ensure the	Yes/ no	yes	Only queried for services that are for processing personal data.

ID	Characteristic	Attribute	Minimum requirement	Remark
	confidentiality, integrity, availability and resilience of systems and services in connection with processing?			
A.5.5.6	Are the availability and access of the data as well as quick recovery in case of a physical or technical incident guaranteed by contract?	Yes/ no	yes	Only queried for services that are for processing personal data.

A.5.6 Transparent price model

Information about used price model, contract duration and notice of cancellation.

Target: Traceable and transparent calculation of services.

Table 25: Transparent price model

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.6.1	Details about used price model	Free text	transparent representation of the price model incl. costs for booking additional cloud capacities	
A.5.6.2	Is the price model publicly available for all customers?	No information, The price model can be provided on demand, The price model is publicly available	The price model is publicly available.	
A.5.6.3	Link to price model	Free text	Mandatory information	Information about link to price model
A.5.6.4	Information about contract duration	Free text	Mandatory information	Several contract durations can be specified.
A.5.6.5	Information about termination modalities and period	Free text	Mandatory information	Several notices of cancellations are specified.
A.5.6.6	Is a free test phase offered?	Yes/ no	Mandatory information	
A.5.6.7	Are the same data privacy requirements applied in the free test phase like in commercial service?	Yes/ no	Mandatory information	A 5.6.7 is requested only if A.5.6.6 was answered with yes.

A.5.7 Change Management

Information of contractual rules for handling changes.

Target: Rules for change management are contractually determined.

Table26: Change Management

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.7.1	Are changes in current contract informed to customers beforehand?	No information, All changes in current contract are informed in advance, All changes in current contract are informed in advance and a special termination right is admitted	All changes in current contract are informed in advance.	This covers all changes for service provision for required subcontractors.
A.5.7.2	Are rules for change management defined contractually?	No information, Rules for change management are not defined in contract, The contract contains clear rules as per which the contract parties can propose and agree	The contract contains clear rules as per which the contract parties can propose and agree during contract duration.	

ID	Characteristic	Attribute	Minimum requirement	Remark
		changes		
A.5.7.3	Description of rules for change management	Free text	Mandatory information	

A.5.8 Obligations to co-operate and provisions of customers

Information about obligations to co-operate and provisions of customers.

Target: Concrete determination of obligations to co-operate, provisions and additional rights of cloud customers.

Table27: Obligations to co-operate and provisions of customers

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.8.1	Are all obligations to co-operate (technical, organizational) and provision of customer defined in contract?	Yes/ no	Provisions and obligations to co-operate are described in contract.	This includes requirements for the customer which in the case of non-compliance can lead to contract ending by the provider.

A.5.9 Copyright and rights of use

Granting of copyright and patent rights for rights of use and indemnification of possible claims of third parties.

Target: Contractual indemnification of the customer from all claims of a third party.

Table28: Copyright and rights of use

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.9.1	Is the customer contractually indemnified from all requirements of a third party within using the service according to contract?	Yes/ no	The customer is contractually indemnified from all requirements of a third party	Especially in reference to used licenses for service provision

A.5.10 Exit support/ support at contract termination

Information about rules for exit support (Exit-Management), especially the adjusted feedback of customer data.

Target: Rules and measures for exit support are contractually defined and described.

Table 29: Exit support/ support at contract termination

ID	Characteristic	Attribute	Minimum requirement	Remark
A.5.10.1	Are rules and measures for exit support contractually defined?	Yes/ no	Rules for exit support are contractually defined.	In the first place is the adjusted feedback of customer data regularized.
A.5.10.2	Description of rules and measures for exit support	Free text	Mandatory information	

A.6 Security

Representation of technical and organizational measures for ensuring data and IT-security.

A.6.1 Security management

Proof of efficient management of information security for example by certification as per ISO 27001 or BSI (IT-basic privacy).

Target: Management of information security takes place as per recognized procedures and is described.

Table 30: Security management

ID	Characteristic	Attribute	Minimum requirement	Remark
A.6.1.1	Is an efficient management of information security ensured, for example as per certification as per ISO 27001/IT-basic protection?	No information, As per recognized procedures, Certified, Certified and reviewed regularly	As per recognized procedures	The proof takes place via filed documentation for mentioned certificate or details about implemented measures.
A.6.1.2	Other details about processes in IT-security management.	Free text	Mandatory information	Information about used ISMS, link to further developing information is possible.

A.6.2 Management of security incidents

Details on the security incident process and emergency management.

Target: Transparent representation of the processes used to report data breaches.

Table 31: Management of security incidents

ID	Characteristic	Attribute	Minimum requirement	Remark
A.6.2.1	Description of the process for reporting data breaches to the client	Free text	Mandatory information	Only queried for services that are for processing personal data.

A.6.3 Security certificates

Information of certificates in area of IT-security.

Target: Proof of implemented measures for IT-security.

Table 32: Security certificates

ID	Characteristic	Attribute	Minimum requirement	Remark

ID	Characteristic	Attribute	Minimum requirement	Remark
A.6.3.1	Name of the certificate	List of specified certificates in A.2.3		Selection list of seal of approval/ certificate of service in A.2.3 for mentioned certificates
A.6.3.2	Other details about certificate regarding scope of test, attributes, extensions etc.	Free text		

A.6.4 Certification of data centers and the technical infrastructure

Information about certificate of data centers and the technical infrastructure.

Target: Proof of implemented measures for ensuring data centers and the technical infrastructure.

Table33: Certification of data centers and the technical infrastructure

ID	Characteristic	Attribute	Minimum requirement	Remark
A.6.4.1	Name of the certificate	List of specified certificates in A.2.3 or A3.3		Selection list of seal of approval/ certificate of service in A.2.3 or A.3.3 seal of approval/ certificate of subcontractor or data centers for mentioned certificates
A.6.4.2	Other details for certificate regarding scope of test, attributes, extensions etc.	Free text		

A.6.5 Encryption

Information about used encryption techniques for encrypting data transmission and storage.

Target: Transparent information on the encryption methods used and the options for key management.

Table 34: Encryption

ID	Characteristic	Attribute	Minimum requirement	Remark
A.6.5.1	Which encryption techniques for encrypting data transmission and storage can be used?	Free text	Mandatory information	
A.6.5.2	Options for key management	No details; Encryption keys are managed by the provider; Encryption keys are managed by the client; Encryption keys can be managed by an external service	Mandatory information	

A.6.6 Identity- and accessmanagement

Information about the rights and roles concept.

Target: Use of a company-wide rights and roles concept.

Table35: Identity- and accessmanagement

ID	Characteristic	Attribute	Minimum requirement	Remark
A.6.6.1	Which rights and roles concept is used?	No information, a company-wide rights and role concept is applied, Other (Free text)	a company-wide rights and role concept is applied	

A.7 Data privacy

Representation of technical and organizational measures for ensuring data privacy and other legal conditions.

A.7.1 Technical and organizational measures

Information about technical and organizational measures for data privacy.

Target: Transparent representation of implemented technical and organizational measures as per German Federal Data Protection Act (BDSG).

Table 36: Technical and organizational measures

ID	Characteristic	Attribute	Minimum requirement	Remark
A.7.1.1	How adequately does the implementation of technical and organizational measures take place by European General Data Protection Regulation (GDPR)?	No information, The measures are formally described, Implementation takes place by written contract for order data agreement acc. Art. 28 GDPR , The measures are certified, The measures are certified and are reviewed regularly	Implementation takes place by contract for order data processing (ODP) agreement	
A.7.1.2	Other details about implemented technical and organizational measures	Free text	Mandatory information	

A.7.2 Formal data privacy requirements

Information of compliance of European data privacy requirements.

Target: Measures to adhere to formal requirements are contractually documented by European General Data Protection Regulation (GDPR).

Table 37: Formal data privacy requirements

ID	Characteristic	Attribute	Minimum requirement	Remark
A.7.2.1	Are the mandatory formal requirements as specified by European General Data Protection Regulation (GDPR) fulfilled?	No information, The information of European General Data Protection Regulation (GDPR)is fulfilled, Measures for fulfillment are documented in contract, Measures for fulfillment are publicly documented, Measures for fulfillment are evident by a certificate	Measures for fulfillment are documented in contract	Main focus on technical and organizational measures
A.7.2.2	Is an ODP contract or legal act agreed with the client based on the EU GDPR requirements?	No information, a written/ electronic ADV contract is not offered,	A written contract according to Art. 28 GDPR is offered	An ODP contract is mandatory when processing personal data. Only queried for services that are for

ID	Characteristic	Attribute	Minimum requirement	Remark
		a written contract is offered, a written/ electronic contract is offered on demand according to Art. 28 GDPR a written/ electronic contract is offered in accordance with Art. 28 GDPR		processing personal data.
A.7.2.3	Is the support of the controller of data protection impact assessment (DPIA) contractually agreed, in case this is necessary for the client? (eg "Data processing on a large scale", "Data transfer outside the EU" etc.)	Yes / no	Mandatory information	Guidelines for creating a DPIA and assessing the risk of data processing can be found in the following document: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Only queried for services that are for processing personal data.
A.7.2.4	Is pseudonymization and/ or encryption of personal data contractually guaranteed?	Yes / no	Mandatory information	Only queried for services that are for processing personal data.
A.7.2.5	Is the application of data subject rights contractually guaranteed?	Yes/ no	Mandatory information	Only queried for services that are for processing personal data.
A.7.2.6	Is the deletion of data including links to the relevant data and data copies in the cloud	yes/ no	Mandatory information	Only queried for services that are for processing personal data.

ID	Characteristic	Attribute	Minimum requirement	Remark
	contractually assured?			
A.7.2.7	Does the ODP contract require information from the client regarding the type of personal data as well as the categories of the persons concerned?	yes/ no	Mandatory information	Only queried for services that are for processing personal data.

A.7.3 Demonstration of compliance

Details on the guarantee of the required proof obligations according to GDPR

Target: The provider can demonstrate the implementation of the obligations laid down in Art. 28 GDPR with appropriate means.

Table 38: Proof requirements

ID	Characteristic	Attribute	Minimum requirement	Remark
A.7.3.1	Which of the following proofs can be provided to the contractor for review by appropriate means in accordance with the ODP contract?	Carrying out a self-audit, internal rules of conduct including external evidence of compliance, Certificate of data protection and/ or	Mandatory details	Only queried for services that are for processing personal data.

ID	Characteristic	Attribute	Minimum requirement	Remark
		information security (eg ISO 27001), approved rules of conduct according to Art. 40 GDPR, Certificates according to Art. 42 GDPR, Other comparable documents/ certificates (Free text)		
A.7.3.2	Is a record of processing activities commissioned by the client based on Art. 30 EU-GDPR created?	yes/ no	yes	See Art. 30 para. 2 GDPR: List of processing activities Only queried for services that are for processing personal data.

A.7.4 Location of data retention

Information about limitation of hosting of customer data to specific regions.

Target: The hosting and the administration of customer data can be limited to specific regions.

Table 39: Location of data retention

ID	Characteristic	Attribute	Minimum requirement	Remark
A.7.4.1	Can the hosting of customer data be limited on a specific location?	No information, The hosting can't be limited to a region, The hosting can be limited to a region, The hosting can be limited to EU, The hosting can be limited to Germany	The hosting can be limited to a region.	Alternative attributes (see Sunyaev/Schneider): 1) The location is outside EU or a contractual state of EEA, but an adequate data privacy level can be ensured for example decision of EU-commission, EU-Standard-contract clauses or confidentiality of corresponding supervisory authorities. 2) The location is outside EU or a contractual state of EEA. 3) The location is within Germany.
A.7.4.2	Can the administration of customer data be limited on a specific location?	No information, The administration of the customer data can't be limited to a specific location, The administration of the customer data can be limited to a location, Can be limited to EU, Can be limited to Germany	The administration of the customer data can be limited to a location.	

ID	Characteristic	Attribute	Minimum requirement	Remark
A.7.4.3	Options of GEO regions	Free text	Mandatory information	Detailed information for options of GEO regions

A.7.5 Implementation of data subject rights

Details on the implementation of the data subject rights in accordance with Art. 12-23 GDPR.

Target: The implementation of the data subject rights in accordance with Art. 12-23 GDPR is ensured by appropriate means.

Table40: Implementation of data subject rights

ID	Characteristic	Attribute	Minimum requirement	Remark
A.7.5.1	How will it be ensured that the requirements of the GDPR for the implementation of the data subject rights, such as eg. the deletion of personal data, are guaranteed?	Free text	Mandatory information	Only queried for services that are for processing personal data.
A.7.5.2	How do you ensure that at the end of the contract, not only the data is deleted, but also links to the data and data copies in the cloud?	Free text	Mandatory information	Only queried for services that are for processing personal data.

A.7.6 Employees data security obligations and awareness

Details on employee commitment to data secrecy.

Target: The obligation of the employees to data secrecy according to Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR is contractually defined.

Table41: Employees

ID	Characteristic	Attribute	Minimum requirement	Remark
A.7.6.1	Is the obligation of all persons authorized to process personal data to be subject to data secrecy according to Art. 28 (3) sentence 2 lit. b, 29, 32 para. 4 GDPR contractually defined?	Yes/ no	yes	Only queried for services that are for processing personal data.

A.7.7 Data privacy certification

Details about available data privacy certifications.

Target: Proof of implemented measures for data privacy by means of a certificate.

Table 42: Data privacy certification

ID	Characteristic	Attribute	Minimum requirement	Remark
A.7.7.1	Name of the certificate	List of specified certificates in A.2.3		Selection list of seal of approval/ certification of services in A.2.3 and specified certificates about it
A.7.7.2	Other details for certificate regarding scope of test, attributes, extensions etc.	Free text		

A.8 Operative processes

Representation of technical and functional prerequisites for use, migration and exchange of service.

A.8.1 Service management

Information about approach in service management.

Target: Proof of an efficient service management for ensuring the quality of service.

Table43: Service management

ID	Characteristic	Attribute	Minimum requirement	Remark
A.8.1.1	Is an efficient service management ensured for example as per ITIL?	No information, The measures are described, As per acknowledged processes, Certified, Certified and regularly reviewed	As per acknowledged processes	
A.8.1.2	Other details for process in service management	Free text	Mandatory information	Description of measures or details about process, link to further developing information

A.8.2 Service management certificates

Details of certificates in the field of service management.

Target: Proof of service quality through appropriate certification.

Table 44: Certificates of service management

ID	Characteristic	Attribute	Minimum requirement	Remark
A.8.2.1	Name of the certificate	List of specified certificates in A.2.3		Selection list of seal of approval/ certification in A.2.3 of the service of specified certificates
A.8.2.2	Other details for the certificate regarding scope of test, attributes, extensions etc.	Free text		

A.8.3 Service availability

Information of ensured service availability in service level agreements.

Target: Transparency of the ensured availability and the maximum expected downtime of services.

Table 45: Service availability

ID	Characteristic	Attribute	Minimum requirement	Remark
A.8.3.1	Ensured service availability in percentage/ year	No information, Availability class 2 99 % ≡ 438 minutes/ month or 7:18:18 hours/ month = 87,7 hours/ year, i.e. 3 days and 15:39:36 hours, Availability class 3 99.9 % ≡ 43:48 minutes/ month or 8:45:58 hours/ year, Availability class 4 99.99 % ≡ 4:23 minutes/ month or 52:36 minutes/ year, Availability class 5 99.999 % ≡ 26.3 seconds/ month or 5:16 minutes/ year, Availability class 6 99.9999 % ≡ 2.63 seconds/ month or 31.6 seconds/ year	Mandatory information	In addition to the proposed availability classes, the availability can be specified freely.
A.8.3.2	Maximum downtime in hours	Free text	Mandatory information	

ID	Characteristic	Attribute	Minimum requirement	Remark
A.8.3.3	How is the quick recovery of availability of client data and access to it guaranteed in the event of a physical or technical incident?	Free text	Mandatory information	Art. 32 GDPR: the ability to quickly recover the availability of personal data and access to it in the event of a physical or technical incident

A.8.4 Backups

Details on backup options and implementation of data protection concepts.

Target: Transparent information to ensure confidentiality during data backup.

Table46: Backups

ID	Characteristic	Attribute	Minimum requirement	Remark
A.8.4.1	Description of backup options	Free text	Mandatory information	
A.8.4.2	How is it ensured that the confidentiality requirements also extend to backups?	Free text	Mandatory information	

A.8.5 Provisioning

Description of types of provision of the service.

Target: Representation of the possibilities of provisioning of the service by the user.

Table 47: Provisioning

ID	Characteristic	Attribute	Minimum requirement	Remark
A.8.5.1	Can the customer provision the service independently?	No information, The service can't be provisioned independently by the customer, The service can be provisioned independently by the customer via web surface, Can be provisioned independently by the customer via web surface and is automatically provided		

A.8.6 Support

Information about support services and documentation.

Target: Transparent representation of ensured support-services of the provider.

Table 48: Support

ID	Characteristic	Attribute	Minimum requirement	Remark
A.8.6.1	Scope/ description of the support-services	Free text	Mandatory information	
A.8.6.2	What is the guaranteed response time of the customer support relating to normal requests?	No information, 4 hours, 1 working day, < 3 working days	< 3 Working days	The time specification is to be understood in consideration of the support times (also see A.8.5.6).
A.8.6.3	What is the guaranteed response time of the customer support relating to critical requests?	No information, 4 hours, 1 working day, < 3 working days	4 hours	The time specification is to be understood in consideration of the support times (also see A.8.5.6).
A.8.6.4	What is average up to time for problem solution related to petty business adverse effects?	No information, < 1 working day, 1 working day,	< 4 working days	

ID	Characteristic	Attribute	Minimum requirement	Remark
		< 4 working days		
A.8.6.5	What is average up to time for problem solution related to critical or relevant business adverse effects?	No information, 1 working day, < 1 working day, < 4 working days	1 working day	The time specification is to be understood in consideration of the support times (also see A.8.5.6).
A.8.6.6	What is the availability of customer support?	No information, normal working hours (5x8), 24/7	Normal working hours (5x8)	
A.8.6.7	Is there complete user documentation?	No information, A complete and updated documentation is available, The documentation is updated regularly and provided to customers, Updated documentation is always available online	A complete and current documentation is available.	This also includes technical documentation for description of offered interfaces (APIs).
A.8.6.8	Is there a complete system documentation?	No information, A complete and current system documentation is available,	A complete and current system documentation is available.	

ID	Characteristic	Attribute	Minimum requirement	Remark
		The system documentation can be made available on demand from the customer.		
A.8.6.9	Are trainings offered?	Yes/ no		
A.8.6.10	Specification of training partners	Free text		More than one training partner can be mentioned.

A.9 Interoperability & portability

Representation of technical and functional prerequisites for use, migration and exchange of service.

A.9.1 Technical standards

Information of technical standards of set service-stacks.

Target: Transparent representation of technical standards on which the service-stack is based.

Table 13: Technical standards

ID	Characteristic	Attribute	Minimum requirement	Remark
A.9.1.1	Is the administration of the	No information,	A web interface is offered	

ID	Characteristic	Attribute	Minimum requirement	Remark
	service possible via standardized APIs or respectively via web interface?	No APIs are offered for administration of the service, A web interface is offered for administration, Documented APIs are offered for administration, Documented and standardized APIs are offered for administration	for administration.	
A.9.1.2	Does the service use standardized formats for virtual machines and container?	No information, The used format is proprietary, The used format is disclosed, A standardized format is used	A standardized format is used.	If requested, then IaaS-offer is handled.
A.9.1.3	Description of standards on which service-stack is based	Free text	Mandatory information	Mandatory information, if IaaS or PaaS-offer is handled.

A.9.2 Data export

Representation of procedures for data access of customer data and data feedback.

Target: Transparency of ensuring data sovereignty of the user.

Table 14: Data export

ID	Characteristic	Attribute	Minimum requirement	Remark
A.9.2.1	Can the user access unlimited and at any time the customer data?	No information, Data export of customer data is initiated after agreement, Data export is possible via a documented API, Standardized APIs are offered	The data export of customer data is initiated after agreement.	
A.9.2.2	Description of procedures for data feedback incl. supported file formats	Free text	Mandatory information	

A.9.3 Integration

Description of procedures for technical integration of the service in the available IT-landscape of the user.

Target: Transparency of integration possibilities of the service in the available IT-landscape.

Table 15: Integration

ID	Characteristic	Attribute	Minimum requirement	Remark
A.9.3.1	Are standardized APIs for integration of the service in the available IT-landscape of the customer offered?	No information, No APIs for service-integration are offered, documented APIs are offered, Standardized APIs are offered	Standardized APIs for service-integration are offered.	
A.9.3.2	Description of offered APIs for integration of the service	Free text	Mandatory information	A.9.3.2. is only requested with corresponding answers at A.9.3.1.

A.9.4 Technical and organizational prerequisites for use of service

Description of technical and organizational prerequisites for use of service.

Target: Transparency in prerequisites for service use which the user must fulfill.

Table 16: Technical and organizational prerequisites for use of service.

ID	Characteristic	Attribute	Minimum requirement	Remark
A.9.4.1	Description of technical pre-requisites for use of service.	Free text	Mandatory information	
A.9.4.2	Description of organizational pre-requisites for use of service.	Free text	Mandatory information	

A.10 Architecture

Description of underlying technical architecture of the service.

A.10.1 Isolation

Description of measures for limiting client areas for dedicated technical infrastructure and data areas.

Target: Transparent representation of implemented measures for isolation of clients.

Table 17: Isolation

ID	Characteristic	Attribute	Minimum requirement	Remark
A.10.1.1	Is a general client separation ensured?	No information, A general client separation is not	A general client separation is ensured.	

ID	Characteristic	Attribute	Minimum requirement	Remark
		ensured, A general client separation is ensured, A general client separation is ensured and is evident by suitable measures.		
A.10.1.2	How does client separation take place?	Free text	Mandatory information for corresponding reply of criterion A.10.1.1	A.10.1.2. is only requested with corresponding answers at A.10.1.1.

A.10.2 Scaling

Information about scaling possibilities of the technical infrastructure.

Target: Representation of the technical infrastructure scalability.

Table 18: Scaling

ID	Characteristic	Attribute	Minimum requirement	Remark
A.10.2.1	Are the scales and factors of the technical infrastructure defined?	No information, The scalability is not defined,	The scalability is defined.	

ID	Characteristic	Attribute	Minimum requirement	Remark
		The scalability is defined, The scalability is defined and ensured by contract		
A.10.2.2	Other information for defining scalability	Free text	Mandatory information	A.10.2.2. is only requested with corresponding answers at A.10.2.1.

5 Change history

This section describes the major changes to each version of the criteria catalog.

5.1.1 Version 2.0

ID	Characteristic	Remark / Change
A.1.1.10	Contact data protection officer acc. Art. 37 para. 5 GDPR or alternative Data privacy contact	At least one data privacy contact has to be specified.
A.1.3.3	Can audits on processes and organizational procedures related to data protection and security be conducted?	New characteristic acc. Art. 28 GDPR
A.2.7.1	What kind of data may be processed?	New characteristic. Defines for which type of data the service is suitable. Possible types are: data without special protection requirements, personal data.
A.4.1.5	Document of the certificate	The upload of the document of the certificate is mandatory.
A.4.1.7	Is the certificate regularly audited?	New characteristic
A.5.2.1	Rights of use	EU contract law is minimum requirement
A.5.2.2	Area of jurisdiction	the area of jurisdiction must be within the EU
A.5.5.5	Is there lasting contractual guarantee to ensure the confidentiality, integrity, availability and resilience of systems and services in connection with processing?	New characteristic acc. Art. 32 para. 1b GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.5.5.6	Are the availability and access of the data as well as quick recovery in case of a physical or technical incident guaranteed by contract?	New characteristic acc. Art. 32 para. 1c GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.6.2.1	Description of the process for	New characteristic acc. Art. 33 para. 2 GDPR

	reporting data breaches to the client	Only queried for services that are for processing personal data. (information on A.2.7.1)
A.6.5.1	Which encryption techniques for encrypting data transmission and storage can be used?	New characteristic acc. Art. 32 para. 1 GDPR
A.6.5.2	Options for key management	New characteristic acc. Art. 32 para. 1 GDPR
A.6.6.1	Which rights and roles concept is used?	New characteristic acc. Art. 32 para. 1 and 2 GDPR
A.7.1.1	How adequately does the implementation of technical and organizational measures take place by European General Data Protection Regulation (GDPR)?	Adaptation acc. Art. 32 para. 1 GDPR
A.7.2.1	Are the mandatory formal requirements as specified by European General Data Protection Regulation (GDPR) fulfilled?	Adaptation acc. GDPR
A.7.2.2	Is an ODP contract or legal act agreed with the client based on the EU GDPR requirements?	New characteristic acc. Art. 28 para. 3 GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.2.3	Is the support of the controller of data protection impact assessment (DPIA) contractually agreed, in case this is necessary for the client? (eg “Data processing on a large scale”, “Data transfer outside the EU” etc.)	New characteristic acc. Art. 35 GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.2.4	Is pseudonymization and/ or encryption of personal data contractually guaranteed?	New characteristic acc. Art. 32 para. 1a GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.2.5	Is the application of data subject rights contractually guaranteed?	New characteristic acc. Art. 28 para. 3e GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.2.6	Is the deletion of data including links to the relevant	New characteristic acc. Art. 28 para. 3g GDPR Only queried for services that are for processing

	data and data copies in the cloud contractually assured?	personal data. (information on A.2.7.1)
A.7.2.7	Does the ODP contract require information from the client regarding the type of personal data as well as the categories of the persons concerned?	New characteristic acc. Art. 28 para. 3 GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.3.1	Which of the following proofs can be provided to the contractor for review by appropriate means in accordance with the ODP contract?	New characteristic acc. Art. 28 para. 3h GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.3.2	Is a record of processing activities commissioned by the client based on Art. 30 EU-GDPR created?	New characteristic acc. Art. 30 para. 2 GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.5.1	How will it be ensured that the requirements of the GDPR for the implementation of the data subject rights, such as eg. the deletion of personal data, be guaranteed?	New characteristic acc. Art. 12-23 GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.5.2	How do you ensure that at the end of the contract, not only the data is deleted, but also links to the data and data copies in the cloud?	New characteristic acc. Art. 28 para. 3g GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.7.6.1	Is the obligation of all persons authorized to process personal data to be subject to data secrecy according to Art. 28 (3) sentence 2 lit. b, 29, 32 para. 4 GDPR contractually defined?	New characteristic acc. Art. 28 (3) sentence 2 lit. b, 29, 32 para. 4 GDPR Only queried for services that are for processing personal data. (information on A.2.7.1)
A.8.3.3	How is the quick recovery of availability of client data and access to it guaranteed in the event of a physical or technical incident?	New characteristic acc. Art. 32 para. 1c GDPR
A.8.4.1	Description of backup options	New characteristic acc. Art. 32 para. 1c GDPR
A.8.4.2	How is it ensured that the confidentiality requirements also extend to backups?	New characteristic acc. Art. 32 para. 1c GDPR

References

[1] Eurocloud Europe, “ECSA Training Material - Part D Catalogue, Version 3.0 Rev 13”,2015.

[2] TÜV Rheinland, “Anforderungskatalog Certified Cloud Service, Version 2.4,” 2014.

[3] ISO / IEC, “ISO / IEC 27001 — Information security management systems — Requirements,” vol. 2013, 2013.

[4] ISO / IEC, “ISO / IEC 27002 — Code of practice for information security controls,” vol. 2013, 2013.

[5] ISO / IEC, *ISO / IEC 27018 — Code of practice for protection of personally identifiable information (PII) in public clouds*, vol. 2014. 2014.

[6] S. Schneider und A. Sunyaev, *Cloud-Service-Zertifizierung*. 2015.

[7] Cloud Security Alliance, “Cloud Controls Matrix, Version 3.0.1,” 2014.

[8] cloud ecosystem, “‘Trust in Cloud’ Check-Liste,” 2011.

[9] Cloud Industry Forum, “The Cloud Industry Forum Cloud Service Provider Code of Practice” 2013.

[10] Bundesamt für Sicherheit in der Informationstechnik, “Sicherheitsempfehlungen für Cloud Computing Anbieter,” *Eckpunktepapier*, S. 93, 2012.

[11] Fraunhofer IAO und CLOUDWerker Konsortium, “AuswahlTable zur Bestimmung sicherheitstechnischer Anforderungen”, 2011.

[12] Bundesamt für Sicherheit in der Informationstechnik und PwC, “Anforderungskatalog für Cloud-Anbieter”, 2015.

[13] Center for Internet Security, “The CIS critical security controls for effective cyber defense,” S. 106, 2014.

[14] Booz & Company und FZI, “Das Standardisierungs- und Normungsumfeld von Cloud Computing - Eine Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms „Trusted Cloud“”, 2011.

[15] M. Hilber und G. Borges, "Leitfaden – Vertragsgestaltung beim Cloud Computing”, Nr. 3, 2014.

[16] Intel, “Intel Cloud Finder”, 2015. [Online]. Verfügbar: https://www.intelcloudfinder.com/.

6 Glossary

Term	Explanation
cloud services	Services (for example data processing, storage capacity) which is available via Cloud Computing. Synonym: cloud offers, cloud applications, cloud solutions
cloud applications	Synonym: cloud services
cloud offer	Synonym: cloud services
cloud provider	Provider of Cloud Computing, cloud offers, cloud services
cloud seal of approval	Seal of approval for cloud services
cloud service provisions	cloud related services which gives out via pure cloud service e.g. consulting service, integration etc.
cloud user	End user/consumer of cloud services.
Label	Synonym: seal of approval
Label Trusted Cloud	Indicates seal of approval to be developed from project „Trusted Cloud“. Synonym: Trusted Cloud seal of approval
Seal of approval	It refers to product which is statement about amicability (quality) of the product. Synonym: Label
Stakeholder	Group of stakeholders who have an interest in the topic or influence the topic (for example associations)
Trusted Cloud Platform	Indicates overall organization of Trusted Cloud. The operation organization and the Trusted Cloud Portal are Part of the Trusted Cloud Platform. The operation organization is responsible for the services of the portal, further development of these and renders additional third party services.

Imprint

Publisher

Federal Ministry for Economic Affairs and Energy
Public Relations
Scharnhorststr. 34-37
10115 Berlin
Post code: 11019 Berlin
V.i.S.d.P. Christina Sasch
Phone: +49 (0)30-18 615-0
Fax: +49 (0)30-18 615-5208

In collaboration with

Kompetenznetzwerk Trusted Cloud e. V.

Lichtstr. 43h
50825 Köln

Phone: +49 (0)221-700048-157
Email: geschaeftsstelle[at]trusted-cloud.de

Web: www.trusted-cloud.de