European Cloud Service
Data Protection Certification

AUDITOR Certification Object

- Draft version 0.4 -

As of 27.03.2019

Related AUDITOR publications:

- criteria catalogue
- concept of protection categories
- DIN SPEC 27557

Online available: www.auditor-cert.eu

Recommended Citation:

Roßnagel, A., Sunyaev, A., Lins, S., Maier, N., & Teigeler, H. (2019). AUDITOR Certification Object – Draft version 0.4. Karlsruhe, Germany: KIT. Online available: www.auditor-cert.eu

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

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

Authors

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

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

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

UNIKASSEL
VERSITÄT

provet

KIT
Karlsruhe Institute of Technology

CRITICAL
INFORMATION
INFRASTRUCTURES
RESEARCHGROUP

Disclaimer

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

Table of contents

List of abbreviations 2

A. Concretisation of the object of certification for the AUDITOR Criteria Catalogue from a legal perspective 3

1. Deriving the object of certification from the General Data Protection Regulation 3

1.1. Legal literature on the object of certification 4

1.2. Data Protection Board guidelines on the object of certification 5

2. Certification object of the AUDITOR certification mechanism 6

B. Details of processing operations of personal data in the context of cloud computing 9

1. Definition of cloud computing and cloud services 9

2. Processing of personal data in the cloud 11

2.1. Definition of personal data 11

2.2. Processing operations in cloud services 12

C. Certification scope and responsibilities 21

1. Layered model to define responsibilities 21

1.1. Explanation layer model 21

1.2. Examples to serve as explanations 22

2. Dividing up responsibilities between the cloud provider and the cloud user 24

3. Dividing up responsibilities between the cloud provider and the sub-processor 25

Bibliography 26

List of abbreviations

Art.	Article
BDSG n.v.	German Federal Data Protection Act new version (applicable as of 25.05.18)
Fig.	Figure
GDPR	EU General Data Protection Regulation (applicable as of 25.05.18)
i.c.w.	in conjunction with
Lit.	litera
No.	Number
Para.	Paragraph
R	Recital
TCDP	Trusted Cloud Data Protection Profile
TOM	Technical and Organisational Measures
w.m.o.	within the meaning of

Note on the gender-neutral wording:

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

A. Concretisation of the object of certification for the AUDITOR Criteria Catalogue from a legal perspective

The object of certification describes the data protection-critical matter to be examined within the framework of AUDITOR on the basis of the certification criteria of the AUDITOR criteria catalogue. A clear definition of the object of certification is important as the subsequent information on the certificate refers to it. Both the cloud providers, as applicants in the certification mechanism, and the cloud users, as customers of the certified cloud service, must be able to rely on the information content. After all, cloud providers want to use the certification to prove their conformity with the General Data Protection Regulation and use it to advertise their products on the market in order to gain a competitive advantage. Through certification, the cloud user wants to be able to trust that the cloud service used is compliant with data protection regulations. After all, the cloud user, as the controller pursuant to Art. 28 para. 1 GDPR, may only cooperate with processors "providing sufficient guarantees" confirming that appropriate technical and organisational measures (TOMs) are implemented in such a manner that the processing will meet the requirements of the General Data Protection Regulation and guarantee the protection of the rights of the data subject.

The first section of the document contains a definition of the object of certification from a legal perspective in accordance with the General Data Protection Regulation. The second section concretises the cloud-specific object of certification from a technical point of view.

1. Deriving the object of certification from the General Data Protection Regulation

Certification mechanisms under data protection law as such have so far been regulated solely by the General Data Protection Regulation. Only Sec. 39 of the Federal Data Protection Act (BDSG) fulfils the regulatory mandate to the Member States in Art. 43 para. 1 sentence 2 GDPR by delegating the accreditation of certification bodies of the German Accreditation Body and the granting of the authority to issue data protection-specific certificates as a certification body to the competent supervisory body. Although the national legislator can also act in the area of certification without an explicit opening clause and provide for its own regulations – provided that they do not contradict the regulations of the General Data Protection Regulation.[1] But this is only the case as long as the national legislator merely specifies indefinite legal concepts,[2] specifies directions that need to be filled out, closes loopholes, or supplements incomplete regulations.[3] Insofar as the General Data Protection Regulation is incomplete, needs to be supplemented or specified, a co-regulation by the national legislator is therefore possible and necessary in order to make the application of the law practicable.[4] As a rule, it is therefore also possible to regulate procedural issues relating to certification in accordance with Art. 42 GDPR in national law in addition to the General Data Protection Regulation. However, such supplementary regulations have not yet been issued.

The General Data Protection Regulation no longer provides for the division between auditing and certification, as was known in German law before.[5] It does not focus on the certification of products or the auditing of data protection management systems.[6] Art. 42 para. 1 sentence 1 GDPR refers only to "data protection certification mechanisms [...] for the purpose of demonstrating compliance of [...] processing operations". According to the wording of the law, complying with the requirements of the Regulation is therefore the standard of review for auditing and thus a "legal implicitness"[7] because the standards of the General Data Protection Regulation are binding anyway, and breaches of duty by the controllers and processors are subject to very heavy fines. There are differing assessments regarding whether certification mechanisms can also include certification criteria that require a higher data protection stand-

[1] *Biervert,* in: Schwarze et al. 2012, Art. 288 TFEU, para. 6; *Roßnagel,* in: Roßnagel 2018, § 2 I, marginal 17.
[2] *Brühann,* EuZW 2009, 643. *Roßnagel,* in: Roßnagel 2018, § 2 I, marginal 17.
[3] *Roßnagel,* in: Roßnagel2018, § 2 I, marginal 17.
[4] *Roßnagel,* in: Roßnagel 2018, § 2 I, marginal 29.
[5] *Hofmann/Roßnagel*, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche 2018, 104; see *Hornung/Hartl,* ZD 2014, 219 et seq.; on the data protection audit *Roßnagel* 2000.
[6] *Bile,* in: Roßnagel 2018 § 5 VII., marginal 237.
[7] *Roßnagel/Richter/Nebel,* ZD 2015, 459; *Bile,* in: Roßnagel 2018, § 5 VII, marginal 238.

ard than that laid down in the General Data Protection Regulation. Partly, a higher standard is considered not to be possible due to the exhaustive nature of the Regulation. [8] Yet some consider that “more” voluntary data protection in certification mechanisms is possible,[9] provided that the additional requirements are in line with the objectives of the Regulation.[10] This view also appears to be supported by the Data Protection Board (Board). Finally, Annex 2 of Guidelines 1/2018 on certification and identification of certification criteria[11] explains that certification mechanisms may not be misleading. Misleading is assumed when, for example, a certification mechanism bears the name “Privacy Gold Standard” but simultaneously contains criteria that only reflect the minimum requirements of the General Data Protection Regulation.[12] It can therefore be concluded that criteria catalogues for certification may also contain criteria that go beyond the statutory minimum requirements of the General Data Protection Regulation. However, this does not play a role in determining the object of certification.

Pursuant to Art. 42 para.1 GDPR, the Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at the Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with the General Data Protection Regulation of *processing operations* by controllers and processors.

However, the term processing operation is not legally defined in the GDPR, while the term processing is. According to Art. 4 para. 2 GDPR, *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, such as 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. At least from the wording of the law it can therefore be concluded, that any handling of personal data must be subject to the audit during certification.

1.1. Legal literature on the object of certification

Before the Board’s guidelines for certification were presented,[13] different views on the object of certification were found in legal literature. On the basis of the wording of Art. 42 para. 1 GDPR, the view was expressed on the one hand that one or more processing operations must be the object of certification, but not the organisation of the controller or processor in its entirety or parts of the organisation.[14] On the other hand, the view was expressed that certifications under Art. 42 para. 1 GDPR are to be regarded as procedural audits and that procedural and process-related processing operations must therefore form the object of certification.[15]

Other views were based on Recital 100, which mentions products and services as the object of certification and stated that holistic certification of products or services is[16] also possible and that certification is not limited to individual processing operations in the technical sense.[17]

This view was countered by the argument that certifications are primarily intended to demonstrate compliance with the General Data Protection Regulation and that therefore only processing operations and not entire products can be connecting factors for an infringement. Therefore, only processing operations could be the object of certification and not products as such.[18] However, according to this view, it should be possible for controllers or processors to certify all processing operations related to the product or

[8] *Hornung/Hartl*, ZD 2014, 224; *Schweinoch/Will*, in: Ehmann/Selmayr 2018, preliminary remarks Art. 40–43, marginal 8.

[9] *Hofmann/Roßnagel*, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche 2018, 106; *Bergt,* in: Kühling/Buchner 2018, Art. 42, marginal 15; *Bile,* in: Roßnagel 2018, § 5 VII, marginal 238.

[10] *Bile,* in: Roßnagel 2018, § 5 VII, marginal 238.

[11] *European Data Protection Board*, Annex 2 on the review and assessment of certification criteria pursuant to Article 42 para. 5 to the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, version for public consultation (hereinafter Annex 2).

[12] *European Data Protection Board*, Annex 2, 9.

[13] *European Data Protection Board,* Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 - revised version after public consultation.

[14] *Schweinoch/Will,* in: Ehmann/Selmayr 2018, preliminary remarks Art. 40–43, marginal 8; *Will,* in: Ehmann/Selmayr 2018, Art. 42, marginal 15; *Eckhardt,* in: Wolff/Brink 2018, Art. 42, marginal 35.

[15] *Hornung*, in: Auernhammer 2018, Art. 42, marginal 46.

[16] *Bergt,* in: Kühling/Buchner 2018, Art. 42, marginal 3; *Eckhardt,* in: Wolff/Brink 2018, Art. 42, marginal 32.

[17] *Bergt,* in: Kühling/Buchner 2018, Art. 42, marginal 3; diff. opinion *by Braunmühl/Wittmann,* in: Plath 2018, Art. 42, marginal 7.

[18] *von Braunmühl/Wittmann,* in: Plath 2018, Art. 42, marginal 7.

service.[19] What should be important is that the object of certification is not a product or a service but that certification is limited to specific processing operations.[20] This should not rule out the possibility that those to be certified only have critical sub-processes certified under data protection law to avoid costs through a certification of undoubtedly uncritical processing operations in accordance with data protection law.[21] This view was shared by parts of the literature to the effect that the controller or the processor could determine the object and scope of the certification themselves.[22]

Other views also went in this direction and came to the conclusion that certifications can cover a "wide range of the scope from individual processing operations" to "parts of processing operations (which can be meaningfully delimited)". For example, a personnel department's applicant data management should be certifiable.[23] From a legal and organisational point of view, the areas of application of certifications should not be restricted either; ergo, neither minimum nor maximum requirements should apply.[24]

1.2. Data Protection Board guidelines on the object of certification

Since January 2019, the guidelines of the Data Protection Board on certification have been available in a revised version after public consultation,[25] containing statements on the object of certification. In its guidelines, the Board remains technology neutral and designates processing operations or bundles of processing operations as the object of certification. It lists three components that must be considered when assessing the object of certification: 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.[26] The Board clarifies that each component of the processing operations in question must be subject to the certification criteria. However, depending on the object of certification, the extent to which they are taken into account may vary. The IT infrastructure supporting the processing operations may be of significance, including the operating system, virtual systems, databases, authentication and authorisation systems, routers and firewalls, storage systems, communication infrastructures or Internet access, associated technical measures and persons involved in the processing operations.[27] It is also made clear that processing operations include organisational measures. The organisational measures may in turn depend on the categories and quantity of personal data processed and the technical infrastructure used. Furthermore, the subject-matter, content and purposes of the processing operation shall be considered within the framework of the organisational measures relating to processing operations, as shall the risks of the processing operation to the rights and freedoms of the data subjects.[28]

The Board's guidelines are also helpful for determining the object of certification because the processing operation term is placed in context with the terms of the standard DIN EN ISO/IEC 17065, which is important for the certification of products and services. It is clarified that processing operations or bundles of processing operations in the terminology of the Regulation lead to a product or service in the terminology of DIN EN ISO/IEC 17065 and can then be the object of a certification.[29]

The Board further makes it clear that any certification scheme may broadly define its object of certification in relation to processing operations or define it in relation to a specific type or range of processing operations. In the case of AUDITOR, these are data processing operations in the context of cloud computing. In any case, the specific processing operations to be covered by the object of certification must be clearly described. This includes the designation of data, processes and technical infrastructures.[30] Interfaces to other processes or services must also be considered and described. Even if, for example, only individual processing operations of a service are to be certified, yet a service consists of several processing operations, then processing operations can only be removed from the object of certification if they have no direct connections to the processing operations that are to be certified. In this case, too,

[19] *von Braunmüh/Wittmann,* in: Plath 2018, Art. 42, marginal 7.

[20] *Laue/Nink/Kremer* 2016, marginal 29

[21] *von Braunmühl/Wittmann,* in: Plath 2018, Art. 42, marginal 7.

[22] *Eckhardt*, in: Wolff/Brink 2018, Art. 42, marginal 34.

[23] *Schweinoch/Will,* in: Ehmann/Selmayr 2018, preliminary remarks Art. 40–43, marginal 9.

[24] *Schweinoch/Will,* in: Ehmann/Selmayr 2018, preliminary remarks Art. 40–43, marginal 8.

[25] *European Data Protection Board,* Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 - revised version after public consultation (hereinafter Guidelines 1/2018).

[26] *European Data Protection Board*, Guidelines 1/2018, marginal 52.

[27] *European Data Protection Board*, Guidelines 1/2018, marginal 53 et seq.

[28] *European Data Protection Board*, Guidelines 1/2018, marginal 56 et seq.

[29] *European Data Protection Board,* Guidelines 1/2018, marginal 55.

[30] *European Data Protection Board*, Guidelines 1/2018, marginal 59.

the connections of the respective processing operations must be described in order to distinguish them clearly and to identify possible data flows between them.[31]

2. Certification object of the AUDITOR certification mechanism

It should be noted that for the AUDITOR certification mechanism, data processing operations in the context of cloud computing, which are performed in cloud services or by (even several) cloud services, form the object of certification.

The fact that certification pursuant to the General Data Protection Regulation does not mean mere product or service certification despite Recital 100, which speaks of "relevant products and services" as the object of certification, is[32] made clear by the purpose of certification. After all, the certification is intended to make it easier for the controllers and processors to provide evidence of various audit and documentation obligations: The certification must be considered "as an element" by which to demonstrate compliance with data protection law pursuant to Art. 24 para. 3 GDPR as well as compliance with the requirements on privacy by design and privacy by default pursuant to Art. 25 para. 3 GDPR. It should also be taken into account when demonstrating sufficient technical and organisational security for processors pursuant to Art. 28 para. 5 GDPR and for the security of data processing pursuant to Art. 32 para. 3 GDPR. In addition, Art. 83 para. 2 lit. j GDPR provides that the supervisory authority must give "due regard" to approved certification mechanisms when imposing fines. Finally, certification can be used to demonstrate the existence of appropriate safeguards for data transfer to third countries in accordance with Art. 46 para. 2 lit. f in connection with Art. 42 para. 1 GDPR.

These articles make it clear that certification under the General Data Protection Regulation must involve an audit of actual data processing against the requirements of the Regulation. Product certification is therefore ruled out because it could only confirm part of the technical and organisational measures of data processing with the controller or processor.[33] After all, the way in which products and services are used by the controller or processor, rather than how they are offered by the manufacturer, is critical. Furthermore, in the case of only a product certification, the General Data Protection Regulation would have to address the manufacturers and not a large number of users, but this is not the case. This is also logical because it would make little sense for controllers and processors as users of an IT product to have the respective product certified multiple times without having sufficient information on it themselves.[34] It would also make little sense if the same product were to undergo the same certification mechanism multiple times at the request of the respective controller or processor.

Rather, certification is intended to establish the conformity of the processing operations performed in products or services or with the help of (even several) products and services with the requirements of the General Data Protection Regulation. They are within the sphere of influence of the controllers and processors and are decisively determined by them, and consequently only the two are named as addressees of certification mechanisms in Art. 42 para. 1 GDPR.

In its guidelines on certification, the Board makes it clear that processing operations can be both technical and non-technical in nature. It therefore includes technology-based and technology-controlled processes and measures, but also organisational ones, which can be of a personnel or manual nature. Organisational measures refer to the circumstances of processing outside and inside technical systems[35] and are to be understood in a broad sense. All types of measures are covered, ranging from those relating to buildings, the security of IT systems, and organisational regulations to access rights, administration, maintenance and measures to implement the principles of privacy by design and by default set out in Art. 25 GDPR.[36] Organisational measures can also interact with technical and automated measures. It should be noted that the General Data Protection Regulation is based on a "dual" understanding of processing operations: A processing operation consists of both non-technical and non-automated and therefore personnel, manual, and organisational processes as well as technical and automated procedures.

[31] *European Data Protection Board*, Guidelines 1/2018, marginal 60.

[32] *Hofmann/Roßnagel*, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche 2018, 106.

[33] Already said by *Hammer/Schuler*, DuD 2007, 79.

[34] *Roßnagel* 2000, 57 et seq.; for old legislation under the BDSG *Roßnagel,* in: Hempel/Krasmann/Bröcking 2011, 267.

[35] *Hartung*, in: Kühling/Buchner 2018, Art. 24, marginal 17; *Martini,* in: Paal/Pauly 2018, Art. 24, marginal 22.

[36] *Hartung*, in: Kühling/Buchner 2018, Art. 24, marginal 17;

Moreover, the Board's guidelines make it clear that individual processing operations within a service can only be certified on their own if they have no direct link to other processing operations of the service. In any case, the specific processing operations to be certified must be described clearly and completely, which also means that interfaces must be described. Individual certification of parts of data processing operations in products or services in the sense of "cherry-picking" uncritical parts and certifying them is therefore not possible under the General Data Protection Regulation. The certification according to Art. 42 and Art. 43 GDPR does, after all, call for a *full confirmation*. This requires that the object of certification be determined in such a way that it has a self-contained procedural structure for the processing of personal data within which the specific data protection risks of the respective data processing operation can be fully recorded.

Certification in accordance with the General Data Protection Regulation must not be misunderstood to mean that the principle of voluntary certification, as set out in Art. 42 para. 3 GDPR, allows for a free determination of the object of certification, as the voluntary aspect is exclusively referring to participation in the certification mechanism and the selection of the specific data processing operation to be certified. Therefore, the cloud provider cannot limit what a data processing operation is and which parts are to be verified to confirm compliance with data protection laws since only self-contained data processing operations can be certified. It is therefore to be recommended for the cloud provider to first create a complete data flow analysis of the application with all actors involved in the processing of personal data, such as other processors (sub-processors),[37] and to determine which data processing steps are to be assigned to the extended area of responsibility of the cloud provider to be certified. It must also be clearly explained how the cloud user's and cloud provider's access options are structured in the respective data processing operations. These internal data processing steps and interfaces must be recorded comprehensively.

In certification practice, certification agreements are concluded with the certification body which identify and clearly define the underlying data processing operations of the cloud service. For the AUDITOR certification process, these are checked by the certification body in the certification mechanism on the basis of the criteria in the AUDITOR criteria catalogue. The processing operations that form the object of certification must comply with all relevant requirements of the General Data Protection Regulation in order to be awarded an AUDITOR certificate. This includes, for example, the definition of processing purposes, the clear definition of responsibilities between cloud users and cloud providers, compliance with all principles of Art. 5 GDPR, the protection of the rights of the data subject and the fulfilment of further safeguards for data transmission outside the European Union and the European Economic Area. All these requirements are laid down as criteria in the AUDITOR criteria catalogue. In the individual certification process, the special features of the respective cloud service models can be considered. This means that though the cloud provider must analyse the data processing operations to be certified in advance, the certification body is involved in the specific application and implementation of the individual certification mechanism and examines it itself.

Cloud services are regularly not provided in their entirety by the cloud provider alone, but sub-processors are used to provide the services. Individual sections or parts of a data processing operation are then delegated to and performed by sub-processors. Assuming the cloud user's consent to using sub-processors, multilevel sub-processing relationships can thus arise, which are very common in cloud computing. Outsourcing data processing to sub-processors must not, however, lead to the specifications of the General Data Protection Regulation being disregarded in the service chain. Rather, the cloud provider, as the main processor, must ensure that the relevant provisions of the General Data Protection Regulation are complied with by all sub-processors at all levels. After all, the cloud provider continues to remain responsible to the cloud user for carrying out the processing. For this reason, the cloud provider must exercise due care when selecting sub-processors and may only cooperate with those who, in accordance with Article 28 para. 1 GDPR, provide "sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." Sub-processors can, for their part, provide the required appropriate safeguards, e.g. by means of a data protection certificate.

[37] Also stated by *EuroPriSe* 2017, paragraph C "the data flow resulting from the use of the product or service is to be illustrated and the legal provisions applicable for the certification are to be determined."

The AUDITOR object of certification

The certification object of the AUDITOR mechanism are data processing operations of personal data performed in products or services or with the help of (several) products or services. The AUDITOR mechanism considers the data processing operations that the cloud provider carries out as a processor as part of processing in accordance with Art. 28 GDPR. Furthermore, those data processing operations are considered that the cloud provider performs as the controller to enter into and perform the contract on the provision of the cloud service with the cloud user or to fulfil legal obligations.

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

Data processing operations must have a self-contained procedural structure for the processing of personal data within which the specific data protection risks of the respective cloud service can be completely considered. This means that interfaces between the data processing operations to be certified and other data processing operations of the service must also be considered in order to identify data flows from which data protection risks may arise. If the data processing operations of a cloud service to be certified are based on platforms or infrastructures not owned by the provider or if the processor uses other sub-processors, the certificate may only refer to those data processing operations that are the responsibility of the respective processor. However, the processor must be convinced that these third-party platforms, infrastructures and sub-processors used by it also comply with the data protection regulations relevant to them and may only use those that comply to provide its service.

B. Details of processing operations of personal data in the context of cloud computing

In order to determine the certification object, a complete data flow analysis, as stated above, including all the bodies involved in the processing of personal data, should be established. Additionally, it must be determined which data processing steps are to be assigned to the extended area of responsibility of the cloud provider. It must also be stated clearly how the access points of cloud users and cloud providers are organised in the respective data processes themselves. In order to support data flow analysis, the second part of this document will detail the processing operations of personal data in the context of cloud computing.

1. Definition of cloud computing and cloud services

There are numerous definitions and explanations of cloud computing in the literature.[38] The definition by the National Institute of Standards and Technology (NIST) has established itself as the standard among experts. According to this definition, cloud computing is a model that enables flexible and demand-based access to a shared pool of configurable computing resources, that can be retrieved at any time and from any location via the Internet or a network.[39] This includes, for example, access to networks, servers, storage or applications. Cloud services are rapidly deployed with minimal management effort and little interaction with the cloud provider and can be customised to meet the needs of cloud users. Furthermore, cloud computing, which is divided into service and deployment models, is characterised by five special features.

Characteristic features of cloud computing include needs-based access, network connectivity, the possibility of resource pooling, high scalability, and usage-based payment: [40]

- **On-demand self-service.** On-demand self-service enables cloud users to independently and almost immediately customise the performance parameters of utilized cloud services. Notably, this can be done automatically and without human interaction with the respective cloud providers. It is thus possible, for example, to increase or decrease obtained computing, storage, or bandwidth capacities, depending on current needs.

- **Broad Network Access.** Cloud services are provided via a broadband network, usually over the Internet. cloud services utilise standardised communication interfaces and can be used with a variety of terminal devices, including smartphones, tablets, and laptops.

- **Resource pooling.** The resources made available by the cloud provider are used simultaneously by multiple cloud users through a multi-client architecture. In the process, the physical and virtual resources are dynamically allocated to different cloud users as needed. Cloud users are not always able to determine the exact location of the utilised resources. However, roughly narrowing down the location in terms of country, region, or data centre is possible in some cases.

- **Rapid elasticity.** Provided resources can be increased or shared flexibly and quickly, in some cases fully automatically, in order to match the resources to the current needs. Among other reasons, this is why the cloud user has the impression that resources seem almost unlimited and are available at any time and to any extent.

- **Measured service.** In order to make cloud services measurable and transparent, cloud services control and optimise resource usage based on service-dependent figures, such as for example, storage space, computing power or bandwidth. Thereby, needs-based billing can be offered and implemented. Furthermore, resource usage is monitored, controlled, logged, and communicated, in order to create transparency with regard to usage for both the cloud user and the cloud provider.

[38] *Leimeister* et al. 2010; *Marston* et al. 2011; *Schneider und Sunyaev* 2015.

[39] *Mell* und *Grance* 2011.

[40] *Mell* und *Grance* 2011; *Sunyaev* und *Schneider* 2013.

Cloud computing differentiates between three basic service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS): [41]

- **Software as a Service (SaaS).** The cloud user can access offered software applications on various devices either via a Thin-Client-Interface, such as a web browser, or via an appropriate application interface. The cloud user has no control over the underlying cloud infrastructure here, but rather can only carry out specific application settings ("user specifics").
- **Platform as a Service (PaaS).** The cloud user can install and operate self-developed or purchased applications on the cloud infrastructure of the cloud provider. To this end, operating systems, databases, programming environments, programme libraries or other services and tools supported by the cloud provider are used. Similar to the Software as a Service model, the cloud user has no control over the underlying cloud infrastructure. On the other hand, the user can manage applications which he/she has installed or carried out and can, if necessary, implement a limited number of settings in the appropriate technical application environment.
- **Infrastructure as a Service (IaaS).** The cloud user gains access to the cloud provider's hardware resources, including computing power, storage capacity, and networks. The user can utilise these resources to install and operate any desired software, such as operating systems or applications. The user is responsible for controlling the operating systems, databases, and installed application, and, if applicable, also selected network resources, such as firewalls, but not the underlying cloud infrastructure.

Furthermore, there are many other service models in practice and the literature, for example, Database as a Service or Security as a Service. These are also often summarised as **Everything as a Service (XaaS).** Still, Only these three basic models will be distinguished in the following.

Furthermore, a distinction is made between the four basic deployment models: private, community, public and hybrid cloud.[42] The provisional virtual-private and multi-cloud models are also often cited in the literature and practice.[43]

- **Private Cloud.** The cloud infrastructure is only used by a single organisation and its members. It can be owned, managed and operated by the organisation, a third party, or a combination of both. Furthermore, the cloud infrastructure does not necessarily have to be local to the organisation. Thus, the private cloud generally serves internal company purposes, and the cloud user has full control over who, how, and when the service can be used.
- **Public Cloud.** The cloud infrastructure can be used by the general public. Companies, academic or government organisations, or a combination of these, own, manage and operate the cloud infrastructure. The public cloud generally provides a selection of services for everyone (e.g., business processes, business practices, applications and infrastructures) on the basis of usage-dependent payment over the Internet at the same time (multi-client capability). One of the most significant distinguishing features of a public cloud is that the cloud user cannot influence (neither technically nor contractually) which other parties use the cloud provider's cloud service. Thus, cloud users (unknowingly or unknowingly in terms of its extent and scope) share the underlying infrastructure, which is, however, completely abstracted from the application layer. Adjusting to specific user requirements is usually only possible to a very limited extent or are subject to the scaling and efficiency interests of the cloud provider.
- **Community Cloud.** The cloud infrastructure is used exclusively by a group of organisations, who have similar demands for the cloud service. One or more organisations of the community, third parties, or a combination of these parties own, manage, and operate the cloud infrastructure. Here again, the cloud infrastructure does not necessarily have to be local to the organisation(s).
- **Hybrid Cloud.** The cloud infrastructure consists of a combination of two, or more, of the above-mentioned models (esp. public and private cloud). The individual infrastructures remain as a unit but are connected by standardised or proprietary technologies. This allows the transfer of data and applications between the connected infrastructures. The purpose of this mixed form of services is to create a solution that best meets the concrete requirements of the respective company.

[41] *Mell* und *Grance* 2011; *Schneider* und *Sunyaev* 2015.

[42] *Mell* und *Grance* 2011; *Schneider* und *Sunyaev* 2015.

[43] *Dillon* et al. 2010; Amazon Web Services 2015.

- **Virtual-Private Cloud.** For the first time, the term "virtual private cloud" was implemented by Amazon Web Services (AWS) when its new product "Amazon VPC" was introduced.[44] In the virtual private cloud model, the infrastructure is provided de facto for an individual organisation that can be comprised of a number of users (for example, business divisions).[45] Access to the cloud service is realised using a Virtual Private Network (VPN). The cloud infrastructure is the property of the Cloud provider. It is operated and managed by the cloud provider, whereby the cloud user maintains complete control of the virtual network environment.
- **Multi-cloud.** If cloud services of different cloud providers are aggregated and combined, this can be referred to as a multi-cloud.[46] Here, cloud providers can voluntarily interconnect their cloud infrastructures and services with other cloud providers, or a cloud broker enters the market, aggregating different cloud services from (different) cloud providers and enabling separate access to them. Figure 1 represents exemplary multi-cloud scenarios. The distinction between a multi-cloud and a hybrid cloud proves to be difficult and inconsistent. In contrast to a hybrid cloud, in which the cloud infrastructures are usually connected and work together (orchestration), in multi-clouds, only certain cloud service components are specifically used by another cloud provider. For example, a multi-cloud provider may perform the computing and network operations in an AWS Cloud, while storage is performed solely by the Azure Cloud.

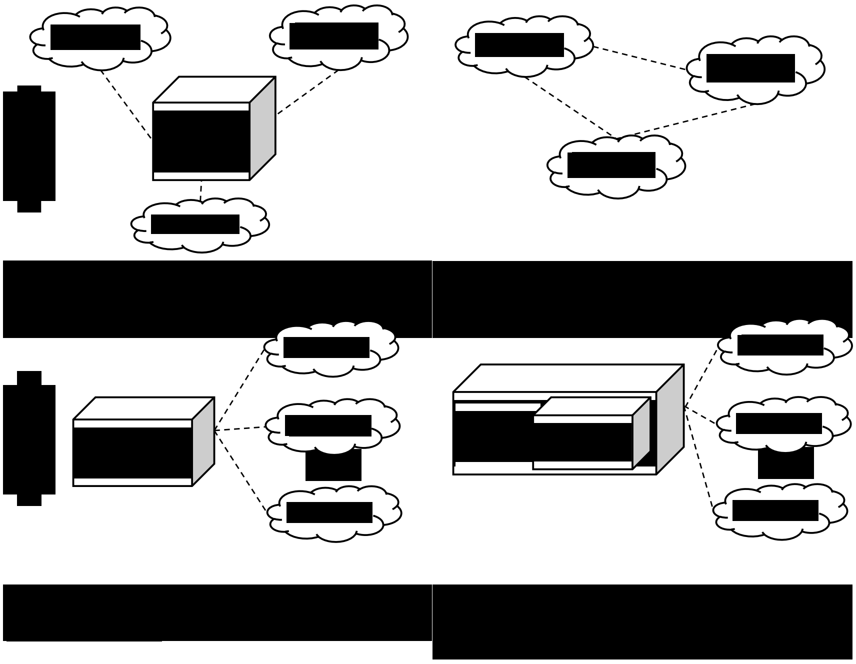


Figure 1. Exemplary types of multi-clouds.[47]

2. Processing of personal data in the cloud

2.1. Definition of personal data

According to Art. 4 No. 1 GDPR, "personal data" refer to any information relating to an identified or identifiable natural person. A natural person is considered to be identifiable if he/she can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Examples:

[44] Amazon Web Services 2015.

[45] *Dillon* et al. 2010.

[46] *Grozev* und *Buyya* 2014.

[47] *Grozev* und *Buyya* 2014.

- general personal data (name, date of birth, age, place of birth, address, email address, telephone number etc.)
- identification numbers (social security number, tax identification number, health insurance number, identity card number, matriculation number, etc.)
- bank details (bank account numbers, credit information, account balances, etc.)
- health-related data
- online data (IP address, location data, etc.)
- physical features (gender, skin colour, hair colour, eye colour, body type, clothing size, etc.)
- ownership/property features (vehicle and real estate ownership, land register entries, license plate numbers, registration data, etc.)
- user data (orders, address data, account data, etc.)
- value judgments (school reports, examination certificates and work certificates, etc.)

2.2. Processing operations in cloud services

The following model graphically represents a reference model for operations in the processing of (personal) data within the context of cloud services. Figure 2 and Table 1 summarise the individual operations of the model. The model is designed to support cloud providers and certification authorities with data flow analysis to identify and classify a data processing operation as a certification object and to define all relevant operations of a series of operations. In addition, it must be individually examined which tasks are to be assigned to the area of responsibility of the cloud provider. General assignment of responsibilities is not possible in the following reference model, since this assignment is heavily dependent on the individual service model and the respective design of the processing agreement made with the cloud user.

When interpreting the model, the following suppositions are taken into account:

1. Not every operation has to be included in a data processing operation that is to be certified.
2. For each operation, the responsibilities must be determined individually, as a cloud provider can outsource an individual or a selection of operations to sub-processors, or responsibilities can fall on the shoulders of the cloud user.
3. Modularisation concepts are not considered in this model.
4. The model makes no claims of completeness.
5. The model does not give any information about conformity to the GDPR. This is determined by the criteria stated in the criteria catalogue.

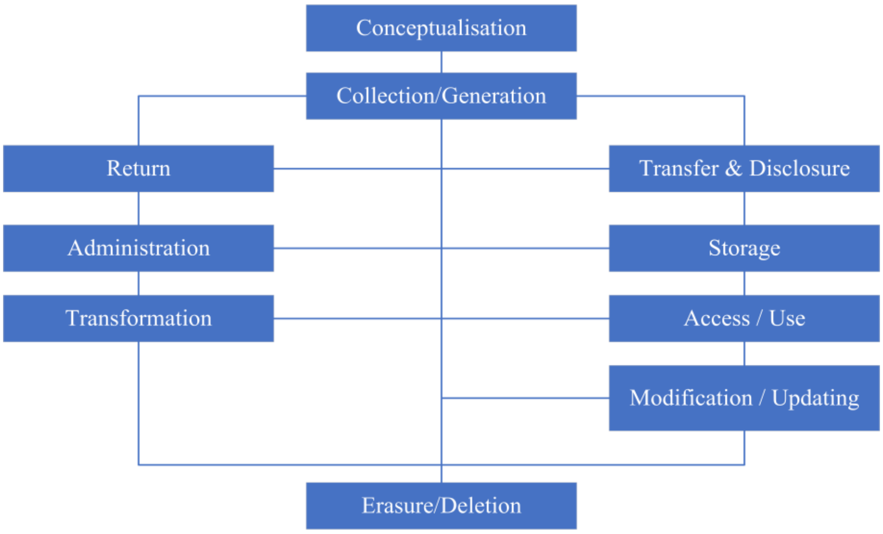


Figure 2. Processing operations model of (personal) data in the context of cloud services to support data flow analysis.

Procedure in data processing	**Description**
Conceptualisation	Definition and description of personal data to be collected and processed.
Collection/Generation	Operations regarding the collection or production of relevant data.
Transfer & Disclosure	Operations that lead to the data reaching their storage or processing location or being disclosed to third parties.
Storage	Operations for secure storage of data.
Access/Use	Read-access to data for further use and processing.
Modification/Updating	Write-access to data to modify the stored values.
Transformation	Purposeful modification of data, particularly for safety reasons.
Administration	Manual and automatic operations relating to the administration of data.
Return	(Complete) return of the data to the cloud user
Erasure/Deletion	Erasure of the data and, if necessary, deletion of the storage mediums.

Table 1. Possible operations of a data processing operation in the cloud.

2.2.1 Conceptualisation

Before a cloud service actually collects and processes data, a cloud provider should check what personal data needs to be collected or generated. While a cloud provider has no or very limited control over which personal data is actually processed in the cloud (e.g., application data of a user), it decides on the data required to operate the service (e.g., identification and billing data of a user).

These personal data to be processed for the operation of the cloud service should be defined and described adequately. This includes, for example, determining the purpose of data processing. Sufficient data conceptualisation supports the subsequent definition of security measures to protect this data and the assignment of roles and responsibilities in data management, among others. In addition, data requirements can also be specified, for example, with regard to quality requirements or necessary meta data. A cloud provider should carry out the conceptualisation process independently of the service model because in principle personal data can be collected and processed for each service model.

2.2.2 Collection/Generation

An initial and central process establishes the collection or generation of personal data.[48] When collecting and generating data, the AUDITOR criteria catalogue distinguishes in particular between **(1) content or application data** that are processed within the scope of as processor and not controller and **(2) personal information and usage data** for which the cloud provider is responsible and which is made available when performing the contract for the provision of cloud services.

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

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

[48] *Higgins* 2008.

tax law so that data processing for the fulfilment of legal obligations also falls within the scope of the AUDITOR certification.

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

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

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

2.2.3 Transfer

When data is collected and subsequently transferred to the cloud infrastructure, for example, to the data centre, appropriate protective measures should be taken.[49] The data transfer includes all operations which ensure that the data reach its storage or processing location.[50] In the context of cloud services, the Internet and Wide Area Network technologies are utilised to transmit the data. This means that well-known hacking attacks, such as IP spoofing, packet sniffer and malware, are relevant in the context of cloud services.[51]

Particularly with the SaaS service model, a cloud provider must specify which directives and measures will be defined and implemented to protect the data during transmission. PaaS and IaaS providers must ensure that offered and open data interfaces (for example, offered databases or virtual machines) are sufficiently secured. In addition, Full-Stack and IaaS providers must monitor and secure transmission within the cloud infrastructure or between dispersed infrastructures. If data are disclosed to intermediaries or third parties, all cloud providers must guarantee that the transmission of data is secure and compliant with data protection requirements. Implementation of a data transfer need not be the responsibility of the cloud provider. It depends on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

SaaS	PaaS	IaaS
Secure collection and subsequent transmission to the cloud infrastructure by, for example, encrypting the communication.	Securing interfaces for data reception or application integration.	Securing interfaces for data reception. Secure data transmission inside and outside the cloud infrastructure, for example, to an external data centre for redundant storage.

Table 2. Data transfer according to the service model.

Significant data transfer operations for cloud services include:

- **Data transfer to the cloud infrastructure via the Internet.** If a cloud service is offered on the Internet, the transmission of collected data usually occurs via the public network. The data must therefore be encrypted when transmitting it in order to avoid possible attacks.

[49] *Higgins* 2008.

[50] *Bernard* 2007.

[51] *Fernandes* et al. 2014.

- **Data transmission to the cloud infrastructure via internal company networks.** When data are transmitted via corporate networks such as WAN, LAN, VPN or similar technologies, the security of transmission must be ensured.
- **Data transfer within the physical cloud infrastructure.** When data are loaded from the hard disk space to memory, swapped between servers, duplicated, or similar operations are performed, it must be ensured that the transfer is secure within a (multi-client capable) cloud infrastructure.[52]
- **Data transfer within a logically separate cloud infrastructure.** On the basis of multi-client capability of cloud services, it may be necessary for data to be transferred between two logically separate networks.[53] Concepts for secure client separation are therefore required.
- **Data transfer between cloud infrastructures.** If a cloud provider owns dispersed cloud infrastructures or data centres and transmits data between them (e.g., due to load balancing or redundant storage), the transmission must be carried out securely.
- **Data transfer between 'cloud federations'.** If cloud infrastructures of different cloud providers are combined, which is referred to as 'cloud federation,' then a defined data exchange takes place between the respective cloud infrastructures and must be secured accordingly.[54]
- **Data transfer to intermediaries.** It is possible for data to be transferred to intermediaries, such as Content Delivery Networks (CDN). For example, Amazon offers a CDN called 'CloudFront' with which content and applications are made available faster and more efficiently. When using intermediaries, particular attention must be paid to ensuring a secure data transfer.

For service provision, it may also be necessary to disclose personal data to third parties. Various scenarios may be possible in this case, such as disclosures to sub-processors who are indispensable for the service provision, disclosures of data as evidence, and to other third parties. The cloud provider should implement appropriate TOMs which ensure that, by default, and thus without active user approval, no personal data are disclosed. Particularly in the case of criminal prosecution, cloud providers may be required to support, for example, a forensic data analysis with the disclosure of user data.[55] The implementation of a data transfer need not be the responsibility of the cloud provider. It depends on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

Significant data transfer operations for cloud services include:

- **Disclosure to sub-processors for service provision.** If sub-processors are involved in the provisioning of services, personal data may be disclosed to them in order to be able to carry out the processing operation.
- **Disclosure to authorised users.** After obtaining consent from the cloud user, collected data may be disclosed to authorised users of the cloud service, for example, by sharing documents with other users.
- **Disclosure to third parties.** After obtaining consent from the data subject, data may also be disclosed to third parties, for example, for advertising purposes.
- **Disclosure to (security) authorities.** Owing to circumstances, data may be disclosed to law enforcement authorities or other government authorities.

2.2.4 Storage

If the data have been transmitted, a large number of processes can be initiated, which will subsequently be reflected upon below.

Preparation of data storage

Various processes can be performed in preparation of data storage. Pursuant to the principle of data economy, after the collection or generation of data, it should be reviewed whether the personal data have to be stored (in the long term).[56] Selecting data for storage reduces storage volume and cost and may reduce potential risks associated with storing sensitive data. A specification of volatile (e.g., DRAM) and non-volatile storage (e.g., HDD) for data storage could be made.

[52] *Jäger* et al. 2016.
[53] *Jäger* et al. 2016.
[54] *Massonet* et al. 2011.
[55] *Fernandes* et al. 2014.
[56] *Higgins* 2012.

Furthermore, meta data (e.g., data format, data storage location or restrictions and requirements for the data) can be defined and stored.[57] Indexing the data would also be a possibility in order to be able to better locate and use the data in the future.[58] Additionally, measures can be taken, which ensure that stored data have a high degree of authenticity, reliability, usability, durability, accuracy and integrity.[59]

The implementation of data preparation operations need not be the responsibility of the cloud provider. It depends on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

Significant data preparation operations for cloud services include:

- **Filtering/Selection.** The cloud service analyses data to be stored and selects actual stored data based on defined criteria in order to meet the requirements of the AUDITOR criteria catalogue, or per the instruction of the cloud user. Discarded data are temporarily stored in volatile data storage locations or safely erased.
- **Generation of meta data for storage.** The cloud service (automatically) generates meta data, which are necessary during storage, for example, to determine the storage location, the size of the data, the access rights or backup intervals.

Implementation of data storage

The personal data are kept on an appropriate storage medium in accordance with security requirements.[60] Depending on the architecture of the cloud service, different databases and storage technologies can be utilised. Additionally, different operations are carried out to assist in storage, including data partitioning. The implementation of data storage need not be the responsibility of the cloud provider. It depends on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

Significant data storage operations for cloud services include:

- **Data indexing.** In order to retrieve data faster, the data are assigned an index according to defined index structures.
- **Data storage on relational databases.** The data are permanently stored in relational databases (e.g., MySQL, PostgresSQL, SQL Server Oracle etc.).
- **Data storage on NoSQL databases.** To achieve increased flexibility and scalability, data can be stored in NoSQL databases (for example, Apache Cassandra, CouchDB, MongoDB etc.).
- **Logical assignment of data.** To secure client separation, logical storage areas can be defined.[61]
- **Data partitioning.** The cloud service splits up the data packages to be stored in order to be able to manage them more efficiently.[62]
- **Data replication.** Data replication describes the copying of data, in order to allow parallel access to said data.[63] Here, a management system must use synchronisation procedures to ensure that any changes to the data are made on all copies.

Data backup

To ensure the availability of stored data, a copy should be made backup. Backups serve to recover files, in case these were manipulated or destroyed, etc. Moreover, redundant data storage is particularly relevant in the sense of cloud services' disaster recovery measures.[64] The implementation of a data backup need not be the responsibility of the cloud provider. It depends on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

Significant data storage operations for cloud services include:

- **Creation of backups.** Data are stored redundantly to increase their availability and reliability. Backups are usually stored in different locations in the case of cloud services.

[57] *Higgins* 2008; *Burton* und *Treloar* 2009; *Curtin* 2010.
[58] *Burton* und *Treloar* 2009)
[59] *Higgins* 2008, 2012.
[60] *Higgins* 2008.
[61] *Jäger* et al. 2016.
[62] *Zhao* et al. 2014.
[63] *Sun* et al. 2012.
[64] *Ofner* et al. 2013.

- **Creation of snapshots.** This includes a stored snapshot of, for example, a system or a database. They support or enable data recovery. However, during the production of snapshots in virtual machines, under certain circumstances, data stored in local or monitoring databases may be deleted accidentally.[65]
- **Data recovery.** Erroneous, manipulated or deleted data are recovered through the utilisation of backups or replicated data and are then made available to the user.

Data archiving

Moreover, data can be archived. Data archives preserve in the long term the originals of older data, which are no longer relevant for daily operation, but are occasionally needed. Data archives are mostly indexed and equipped with a search function in order to be able to retrieve data, completely or partially. The implementation of data archiving need not be the responsibility of the cloud provider. It depends on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

Significant data archiving operations for cloud services include:

- **Review of archivability.** An ongoing process whereby data are reviewed with regard to the defined archiving criteria that trigger archiving. This means that data which has remained unused for a long period of time could be archived.
- **Copy data from the database to the archive.** If the review for archivability is successful, data are moved to the archive and the previously occupied storage space is freed up.
- **Access to data in the archive.** Access to archived data may become necessary.
- **Delete data from the archive.** Archiving over several years leads to an immense amount of data, which should be handled by deleting said data according to defined retention periods.

Migration of stored data

The concept of data migration is multifaceted. On the one hand, data migration includes the conversion of data formats, which, for example, are a result of the change in underlying technologies, software or hardware.[66] On the other hand, data migration describes the process of changing the data storage location.[67] Especially in the cloud computing environment, the storage and processing location of (personal) data are flexible and can usually be changed without much effort, for example, on the grounds of load balancing, the availability of (redundant) data centres or flexible storage costs.[68] For this reason, suitable guidelines must be established for the migration of (personal) data within the cloud infrastructure. The implementation of a data migration need not be the responsibility of the cloud provider, depending on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

Significant data migration operations for cloud services include:

- **A change of the data storage location.** Within the realm of load balancing, a malfunction, or other reasons, a cloud service can change the location of data and migrate said data to another data centre.
- **A change of the data format.** Changing the underlying technologies, software, hardware, or data models may require modifying the data formats. While changing data formats, personal data may also be processed. For example, it may be necessary for personal data to be converted to a JSON format and to be stored in an XML format.

2.2.5 Access/Use

A further central process is the read-access to the data. In this case, for example, access by a cloud user to his own data can be distinguished from access by the cloud provider for further processing of the data. To ensure secure access to personal data, adequate identity and access management systems, in addition to guidelines, are required.[69] Data access management need not be the responsibility of the cloud provider. It depends on the respective service model, as well as the design of the cloud service and the individual processing agreement made with the cloud user.

[65] *Pearce* et al. 2013.

[66] *Higgins* 2008.

[67] *Michener* und *Jones* 2012; *Alatorre* et al. 2014.

[68] *Alatorre* et al. 2014.

[69] *Higgins* 2008.

Significant data-access operations for cloud services include:

- **Access verification.** Before access to data can be granted, several identification, authorisation and authentication procedures must be carried out. As part of this review, entered personal data are compared with the data stored in the system.
- **Finding the data.** In order to find the requested data, search operations can be performed which, if need be, access a large number of personal data before the requested data are found.
- **Read-access by the cloud user.** The cloud user, or an individual authorised by him, initiates access to his data, which are subsequently displayed or provided by the cloud service (for example, via an interface).
- **(Automatic) read-access by the cloud service to perform the processing operation.** As part of the primary processing operation, a cloud service can access the data, for example, to read it and subsequently use it for processing.
- **(Automatic) read-access by the cloud service to perform other operations.** A cloud service can also access personal data to carry out secondary or supporting operations. This includes, among other things, monitoring or internal auditing procedures.
- **(Manual) access by employees of the cloud provider.** Employees of the cloud provider may have read-access to personal data (application data), for example, within the scope of support activities.
- **Read-access by third parties.** After obtaining consent from the cloud user, data may also be retrieved and used by third parties, for example, through defined interfaces in an application.

2.2.6 Change within processing

In addition to the mere read-access of the personal data, they can be changed or updated, for example, due to user actions or processing results. Here, it is therefore not a reading-process, but a writing-process that actively changes the existing data.[70] The management of data changes need not be the responsibility of the cloud provider. It depends on the respective service model, as well as the design of the cloud service and the individual processing agreement made with the cloud user.

Significant data alterations for cloud services include:

- **Changes by the cloud user.** The cloud user, or an individual authorised by him, changes or updates personal data, for example, in the course of changing an address.
- **(Automatic) changes by the cloud service.** Data stored in the cloud may be changed by the cloud service within processing operations, such as changing a user's location data.
- **(Manual) changes by employees of the cloud provider.** Employees of the cloud provider may theoretically carry out changes to data (application data), for example, within the scope of support activities.
- **Changes by third parties.** Changes/processing by third parties, insofar as there is a legal basis to do so, for example, consent from the person concerned.

2.2.7 Transformation

In addition to the modification of personal data in the context of the actual processing, these can also be purposefully transformed by secondary or support processes. This includes, for example, transformation processes such as filtering, harmonisation, synthesis, aggregation and enhancement. Above all, transformations play an important role in data protection. This includes, in particular, encryption, pseudonymisation and anonymisation processes. The implementation of data transformations need not be the responsibility of the cloud provider, depending on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

Significant data transformations for cloud services include:

- **Data cleansing.** Data cleansing can be carried out, for example, to correct or delete data errors from the database. These errors can result, for example, from incorrect, outdated, or inconsistent data.
- **Data sorting.** Data can be put into order according to defined criteria.
- **Data mapping.** Mapping and transforming data between different data models.
- **Data conversion.** Data conversion describes the change in the data format and includes, for example, changing the selected character format from UTF-8 to UTF-16.
- **Aggregation.** Aggregation describes the summary of data, i.e., the summation.

[70] *Möller* 2013; *Higgins* 2008.

- **Integration.** The merging of data from different sources into one data set.
- **Linkage.** The logical linkage of data creates a relationship between data from different sources.
- **Encryption.** The conversion of a plain text, by means of a key and an encryption algorithm, into an encrypted text ('ciphertext').
- **Anonymisation.** Anonymisation is the modification of personal data in such a way that it can no longer, or only with a disproportionate amount of time, money and effort, be ascribed to a specific or identifiable natural person.
- **Pseudonymisation.** According to Art. 4 No. 5 GDPR, pseudonymisation is described as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

2.2.8 Administration

Furthermore, processes to manage data can be established. This includes, for example, quality assurance measures that are (manually) performed and ensure high data quality,[71] or administrative activities based on instructions from the cloud user. Directives must be created, which determine the administration of data.[72] Administrative operations are highly sensitive especially in the context of cloud services since an administrator can, for example, cause a loss of data due to an error during data migration or while creating backups.[73] The administration of data need not be the responsibility of the cloud provider, depending on the respective service model and the design of the cloud service and the individual processing agreement made with the cloud user.

- **Administration of application data.** Cloud user support queries allow administrators of the cloud provider to manage application data, such as recovering data or launching virtual machines.
- **Review/Tracking of data movements.** Automated or manual processes to review and analyse data traces can be performed to guarantee data locality requirements.
- **Data verification.** Automated or manual processes can be performed to verify the accuracy of personal data; for example, verifying that the entered postal code corresponds to the location.
- **Identification of data anomalies.** To ensure data quality, automated or manual administration operations can be performed, which, for example, identify and resolve read-write conflicts, data inconsistencies, insertion anomalies, update anomalies, and deletion anomalies.
- **Correction of data.** Administrative correction of data can be performed, for example, in order to, correct or delete data errors from the databases. These errors can result, for example, from incorrect, outdated, or inconsistent data.

2.2.9 (Complete) return of data

At the end of the contractual period of the data processing or at the request of the cloud user, there are operations that can be initiated which carry out a (complete) return of the data. This is also known as backsourcing. Especially in the cloud computing environment, the portability of data is paramount for data return processes. Thus, it is required that the transmission of personal data is carried out in a structured, conventional and machine-readable format. Managing returning data need not be the responsibility of the cloud provider. It depends on the respective service model, as well as the design of the cloud service and the individual processing agreement made with the cloud user.

- **Automated data export.** The cloud service automatically identifies all relevant data sets and transforms these into a defined format (e.g., XML, CSV or JSON) so that the data sets can be exported via an export interface (e.g., API or download tool).
- **Manual data export.** An administrator extracts all data and transmits or transfers them to the cloud user.

2.2.10 Erasure/Deletion

The final step in data processing is the permanent deletion of personal data.[74] This can be done particularly at request by the cloud user. With regard to cloud services, it should be noted that permanent and

[71] *van Veenstra* und *van den Broek* 2015; *Michener* und *Jones* 2012.

[72] *Ofner* et al. 2013.

[73] *Fernandes* et al. 2014.

[74] *Higgins* 2008; *Bernard* 2007.

complete deletion requires special attention, among other reasons, on account of multi-client architecture, resource bundling, data redundancy and the distributed systems.[75] Conclusive, physical destruction/deletion of storage media may be required. Data deletion need not be the responsibility of the cloud provider. It depends on the respective service model as well as the design of the cloud service and the individual processing agreement made with the cloud user.

- **Data clearing.** Data clearing includes all logical techniques for the erasure of all storage mediums containing personal data. Usually simple techniques are utilised here, such as the iterative description of the medium with an order of 0 and 1. Data clearing is only effective against simple and non-invasive data recovery methods.
- **Data purging.** Data purging involves physical or logical, state-of-the-art techniques that make data recovery impossible.
- **Data destruction** Data destruction involves physically destroying the storage medium so that it cannot be reused. This includes, for example, melting the storage medium.
- **Erasure of primary data.** All primary data of the cloud user should be erased, including, among others, application data which are required for data processing.
- **Erasure of secondary data.** Furthermore, all secondary data of the cloud user should be erased. This includes, in particular, backups, replications or meta data.

[75] *Pearson* und *Benameur* 2010.

C. Certification scope and responsibilities

For certification according to AUDITOR, the certification scope as well as the field of application must be clearly defined. Of importance here are the identification and definition of responsibilities of the cloud provider, by the cloud users and sub-processors.

1. Layered model to define responsibilities

1.1. Explanation layer model

Cloud computing is based primarily on an interlaced value-added network, which is understood as a layered architecture ('cloud stack'). This layered architecture also mirrors the various cloud computing service models. Based on the cloud stack, the potential influences for the cloud provider, the cloud user, as well as possible sub-processors can be determined. Table 3 schematically outlines the potential influences. Depending on the architecture of the cloud service, deviations may occur in practice. Moreover, a cloud service is not limited to a specific operation environment or layer. The layers can be spread out across all levels and, in the sense of the networked service structure, can be operated simultaneously by legally independent sub-processors. Thus, different parties and a combination of parties (for example, cloud providers and sub-processors) can be responsible for platform security.

Party	IaaS	PaaS	SaaS	Description of the layer
Cloud user(s)	Secure application usage	Secure application usage	Secure application usage	The cloud user is responsible for secure/safe usage of the application.
	User specifics	User specifics	User specifics	User-specific settings or configurations of used applications.
	Application	Application	Application	Offered software solutions.
	Software security	Software security	Software security	Mechanisms to increase the security of provided applications.
	Administration and support of the software	Administration and support of the software	Administration and support of the software	Administration of the software on offer, as well as receipt and handling of support inquiries from the cloud user.
	Operating system	Operating system	Operating system	Basic software for operation of the application.
	Runtime environment	Runtime environment	Runtime environment	The runtime environment carries out applications for which the runtime environment is suitable.
	Database	Database	Database	Software for the management and structuring of data.
	Platform security	Platform security	Platform security	Mechanisms to increase the security of provided applications.
	Administration and support of the software	Administration and support of the software	Administration and support of the software	Administration of the provided platform, as well as receipt and handling of support inquiries from the cloud user.
	Virtual machines	Virtual machines	Virtual machines	Virtual representation of computer resources like, for example, servers or CPUs.
Cloud provider	Virtualisation layer	Virtualisation layer	Virtualisation layer	Mechanisms for the creation and management of virtual machines.
	Calculation components	Calculation components	Calculation components	Components to conduct calculations or processing of data in the cloud service.
	Storage	Storage	Storage	Mechanisms for the storage of data.
	Network	Network	Network	Mechanisms for the transfer of data.
	Infrastructure security	Infrastructure security	Infrastructure security	Mechanisms to increase the security of provided resources.
	Administration and support for the infrastructure	Administration and support for the infrastructure	Administration and support for the infrastructure	Administration of the provided infrastructure, as well as receipt and handling of support inquiries from the cloud user.
	Hardware			The physical hardware for operation of the cloud service.
	Premises, set-up and equipment			The physical set-up of the could service.
	Connectivity and network connection			Physical connectivity of the data centre.
	Data centre security			Mechanisms to increase the security of the data centre, including parties responsible for the premises, with security staff and physical security systems.

Table 3. Potential influences according to the layer model.[76]

When using a SaaS service, the cloud user generally lacks the technical possibility to make alterations within the cloud service. The only possibility is for a cloud user to be able to implement certain configurations or settings on related cloud applications, such as turning certain features on or off, or customising graphical user interfaces. Furthermore, it should also be noted that the cloud user is responsible for using the cloud application securely and compliantly. The core business of the SaaS provider includes the development, operation and administration of the software application, as well as ensuring software

[76] Adpted from *Singh* et al. 2016; European Network and Security Agency 2012.

security. The remaining cloud layers are the responsibility of the SaaS Cloud provider (full-stack provider) or are outsourced to a sub-processor.

In the case of a PaaS service, a cloud user runs his/her own applications on a provided cloud platform. Thus, the cloud user is responsible for the creation and operation of the applications. Additionally, the cloud user must answer for the security of the application, for example, in order to prevent cross-site scripting or software flaws. The core business of the PaaS provider includes the development, operation and administration of the platform (e.g., the provided systems or databases), as well as ensuring platform security. The remaining cloud layers are the responsibility of the PaaS cloud provider (full-stack provider) or are outsourced to a sub-processor.

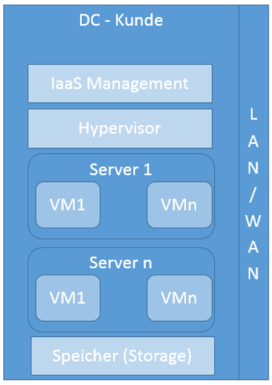
The cloud provider of the IaaS service is responsible for the correct and secure virtualisation and the provision of the necessary physical resources. A cloud user is responsible for leased virtual machines and the applications, databases, operating systems, and runtime environments used thereon. In addition, the cloud user assumes responsibility for software and platform security. The required physical hardware, set-up and equipment can be provided by an IaaS provider (full-stack provider) or can be obtained from a sub-processor's data processing centre.

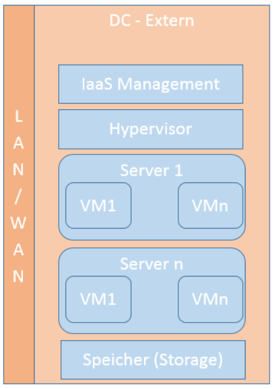
Depending on the specific design of the cloud service and the processing agreements made with cloud users, different responsibilities may arise. Regarding further literature, reference is made to the NIST '*Cloud Security Reference Architecture'*, which lists a detailed perspective of the potential influences on the various service models. This can be found in Appendix D (NIST Cloud Computing Security Working Group 2013).

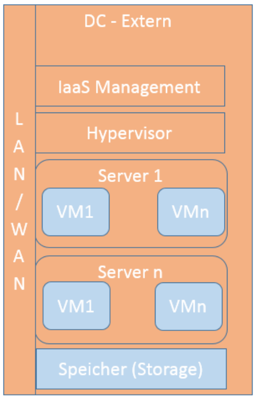
1.2. Examples to serve as explanations

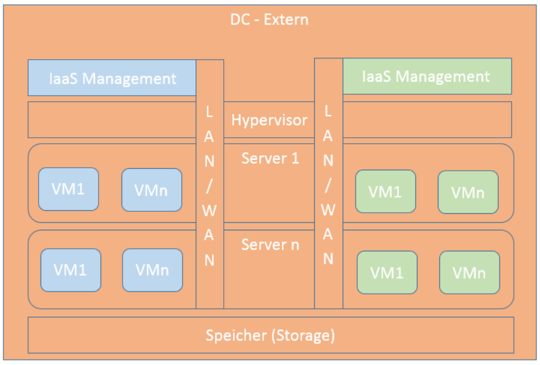
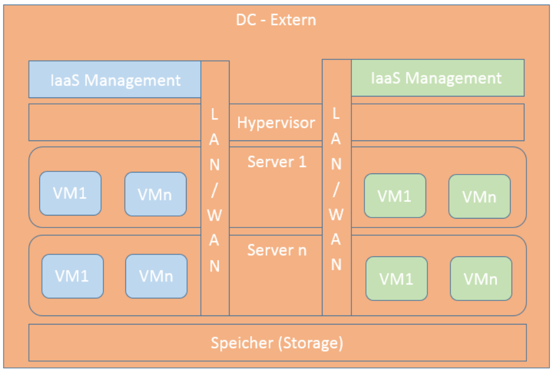
In the following text, several different service models (IaaS, PaaS and SaaS), in combination with deployment models (private and public), will be described. The constellation of one or more external cloud providers working together in the context of the service provision is to be considered in more detail. Labels of different colours are used to illustrate the respective areas of responsibility for the cloud user and the cloud provider.

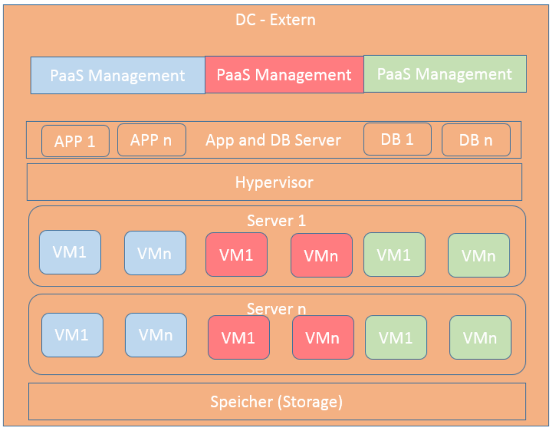
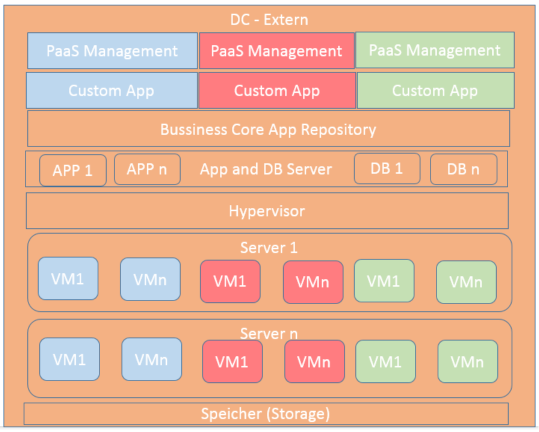
<table>
<tr><th>Private Cloud – On Premise</th><th>Private Cloud – Externally Hosted</th><th>Private Cloud – Externally Managed</th></tr>
<tr>
<td>In the case of "Private Cloud On Premise," it is assumed that the entire technical infrastructure can be completely and immediately controlled by the cloud user.

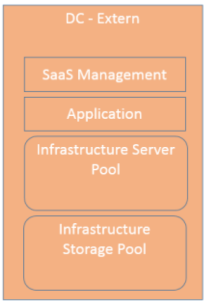
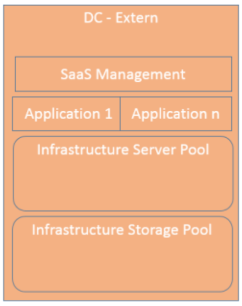
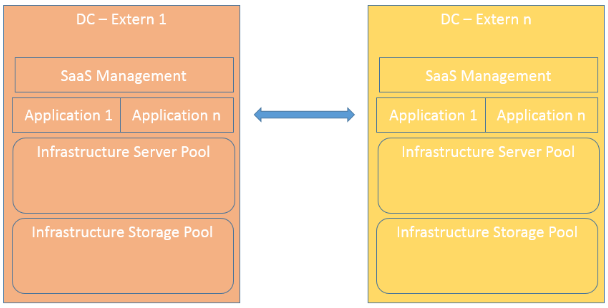

</td>
<td>In "Private Cloud Externally Hosted," the structure of the technical environment is provided by a cloud provider (DC CoLocation, WAN, IX), while the IT systems (server, storage, local switch, LAN) belong to the cloud user. Additional services (hands-on services, access control systems, system monitoring) are usually arranged with the cloud provider.


</td>
<td>Complementary to "Private Cloud Externally Hosted," the technical support of the system is taken over by the cloud provider with direct access to both the system and the data.


</td>
</tr>
<tr><td colspan="3">* <i>Blue: Primarily the responsibility of the cloud user</i>
<i>Orange: Primarily the responsibility of the cloud provider</i></td></tr>
</table>

Virtual Private Cloud IaaS	Public Cloud IaaS
The Virtual Private Cloud is a special variant of the Public Cloud. A logical separation at the infrastructure level (LAN, SAN, dedicated Virtual Hosts) enables a specific client assignment for the dedicated use of a cloud user.  DC - Extern IaaS Management IaaS Management LAN/WAN Hypervisor Server 1 LAN/WAN VM1 VMn VM1 VMn Server n VM1 VMn VM1 VMn Speicher (Storage)	In the Public Cloud IaaS, all infrastructure resources are provided by means of dedicated booked virtual servers from a total pool of technical servers. Storage capacities are dynamically assigned from available storage pools (SANs) and allocated for the booking duration.  DC - Extern IaaS Management IaaS Management LAN/WAN Hypervisor Server 1 LAN/WAN VM1 VMn VM1 VMn Server n VM1 VMn VM1 VMn Speicher (Storage)
** Blue: Primarily the responsibility of the cloud user* *Orange: Primarily the responsibility of the cloud provider* *Green: Responsibility of other cloud users*	

Public Cloud PaaS – Core Packaged	Public Cloud PaaS – Core Business App
The Public Cloud PaaS - Core is an extension of a Public Cloud IaaS to facilitate standardised operating system services and application services (databases, app and web servers, IDM) which enable a coordinated management.  DC - Extern PaaS Management PaaS Management PaaS Management APP 1 APP n App and DB Server DB 1 DB n Hypervisor Server 1 VM1 VMn VM1 VMn VM1 VMn Server n VM1 VMn VM1 VMn VM1 VMn Speicher (Storage)	The Public Cloud PaaS - Core Business App is a SaaS basic preliminary stage for application services, which can be customised to accommodate special needs via direct programming. These additional models are provided as isolated applications in the Public SaaS model.  DC - Extern PaaS Management PaaS Management PaaS Management Custom App Custom App Custom App Bussiness Core App Repository APP 1 APP n App and DB Server DB 1 DB n Hypervisor Server 1 VM1 VMn VM1 VMn VM1 VMn Server n VM1 VMn VM1 VMn VM1 VMn Speicher (Storage)
** Blue: Primarily the responsibility of the cloud user* *Orange: Primarily the responsibility of the cloud provider* *Green, red: Responsibility of other cloud users*	

Public Cloud SaaS – Single	**Public Cloud SaaS – Suite**	**Public Cloud Multi SaaS – Suite**
The Public Cloud SaaS - Single allows for a dedicated multi-client application to be provided for public use.  DC - Extern SaaS Management Application Infrastructure Server Pool Infrastructure Storage Pool	The Public Cloud SaaS - Suite allows for a logical group of multi-client-capable applications to be provided for public use.  DC - Extern SaaS Management Application 1 Application n Infrastructure Server Pool Infrastructure Storage Pool	The Public Cloud Multi SaaS - Suite allows for a logical group of multi-client-capable applications to be provided for public use over several Saas providers.  DC – Extern 1 SaaS Management Application 1 Application n Infrastructure Server Pool Infrastructure Storage Pool DC – Extern n SaaS Management Application 1 Application n Infrastructure Server Pool Infrastructure Storage Pool
** Orange: Primarily the responsibility of the cloud provider* *Yellow: Primarily the responsibility of another cloud provider*		

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

It is not uncommon that cloud computing regularly leads to a coexistence of responsibilities between the cloud provider and the cloud user. General guidelines on the division of responsibilities are difficult to formulate since the distribution of responsibilities largely depends on the service models and the specific designs as well as the individual processing agreements with the cloud users. It is therefore up to the cloud user and the cloud provider to determine rules for distributing responsibilities. For example, the cloud user is usually responsible for data backups or archiving. As a result, most processing agreements between IaaS providers and cloud users will include an appropriate regulation of responsibilities.

The regulations must reflect the intentions and objectives. When it comes to the relationship between the cloud user and the cloud provider, the cloud provider is always the contractor where it does not pursue its own purposes with the data to be processed, even if it makes decisions about the means of data processing. The cloud provider is only the controller if it pursues its own purposes with the data. The cloud provider will remain the processor, however, when the cloud user clearly defines the processing purpose but leaves the decision-making power as regards the choice of technical and organisational means to the cloud provider, insofar as such means are suitable for achieving the purposes of the processing, and the cloud provider informs the cloud user thereof.[77]

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

[77] *Art. 29 Working Party*, WP 169, p. 17 et seq.

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

As shown,[78] the cloud provider can also use sub-processors to provide its cloud service. If it chooses this option, however, it must ensure that the requirements of the General Data Protection Regulation are also complied with in this service chain. The cloud provider, as the main processor, must ensure that the relevant provisions of the General Data Protection Regulation are complied with by all sub-processors at all levels.

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

If a cloud provider is itself part of a cloud service consisting of multiple data processing operations, it will generally only have its clearly defined data processing operation, for which it is responsible, certified. It is important to note that such a "domain certification" enables recognition as part of higher-level certification mechanisms.

[78] Cf. Chapter A, 2.

Bibliography

Alatorre, Gabriel; Ayala, Richard; Chavda, Kavita; Gopisetty, Sandeep; Singh, Aameek, Data lifecycle management within a cloud computing environment. Angemeldet durch International Business Machines Corporation. Veröffentlichungsnr: US8918439 B2, 2014.

Amazon Web Services, AWS | Amazon Virtual Private Cloud (VPC) – Sichere private Cloud (VPN), 2015.

Bernard, Ray, Information Lifecycle Security Risk Assessment. A tool for closing security gaps. In: Computers & Security 26 (1), 2017, 26–30. DOI: 10.1016/j.cose.2006.12.005.

Bile, Tamer, § 5 VII. Zertifizierung, in: Roßnagel, Alexander (Ed.), Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Baden-Baden 2018, 211-220.

Brink, Stefan, Wolff, Amadeus (Ed.), BeckOK Datenschutzrecht, 24. Edition, München 2018.

Brühann, Ulf, Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG, Zugleich ein Beitrag zur Systematik von Richtlinien zur Rechtsangleichung im Binnenmarkt in der Rechtsprechung des Europäischen Gerichtshofs, Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2009, 639-644.

Burton, Adrian; Treloar, Andrew, Designing for Discovery and Re-Use. The 'ANDS Data Shar-ing Verbs' Approach to Service Decomposition. In: IJDC 4 (3), 2009, 44–56. DOI: 10.2218/ijdc.v4i3.124.

Curtin, Gregory G., Free the Data!: E-Governance for Megaregions. In: Public Works Management & Policy 14 (3), 2010, 307-326. DOI: 10.1177/1087724X09359352.

Dillon, Tharam; Wu, Chen; Chang, Elizabeth (Ed.), Cloud Computing: Issues and Challenges. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA 2010). Perth, Australia.

Ehmann, Eugen, Selmayr, Martin (Ed.), DS-GVO, Datenschutz-Grundverordnung Kommentar, 2. Auflage, München 2018.

European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, revised version after public consultation, 2019, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en, zuletzt ab gerufen am: 1.3.2019.

European Data Protection Board, Annex 2 on the review and assessment of certification criteria pursuant to Article 42(5) to the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 ans 32 of the Regulation 2016/679, Version for public consultation, 23.1.2019 abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-0_en, zuletzt abgerufen am: 1.3.2019.

European Network and Security Agency, Cloud Computing - Benefits, Risks and Recommendations for Information Security, 2012.

EuroPriSe, Criteria for the certification of IT products and IT-based services (v201701), 2017, abrufbar unter: https://www.european-privacy-seal.eu/EPS-en/Criteria, zuletzt abgerufen am 12.9.2018.

Fernandes, Diogo A. B.; Soares, Liliana F. B.; Gomes, João V.; Freire, Mário M.; Inácio, Pedro R. M., Security issues in cloud environments. A survey. In: Int. J. Inf. Secur. 13 (2), 2014, 113–170. DOI: 10.1007/s10207-013-0208-7.

Grozev, Nikolay; Buyya, Rajkumar, Inter-Cloud architectures and application brokering. Taxonomy and survey. In: Softw. Pract. Exper. 44 (3), 2014, 369–390. DOI: 10.1002/spe.2168.

Hammer, Volker/Schuler, Karin, Cui bono? – Ziele und Inhalte eines Datenschutz-Zertifikats, Datenschutz und Datensicherheit (DuD) 2007, 77-83.

Higgins, Sarah, The DCC Curation Lifecycle Model. In: IJDC 3 (1), 2008, 134–140. DOI: 10.2218/ijdc.v3i1.48.

Higgins, Sarah, The lifecycle of data management. In: Graham Pryor (Hg.): Managing Re-search Data. London: Facet Publishing 2012.

Hofmann, Johanna/Roßnagel, Alexander, Rechtliche Anforderungen an Zertifizierungen nach der DSGVO, in: Krcmar, Helmut/Eckert, Claudia/Roßnagel, Alexander/Sunyaev, Ali/Wiesche, Manuel (Ed.), Management sicherer Cloud-Services, Entwicklung und Evaluation dynamischer Zertifikate, Wiesbaden 2018, 101-112.

Hornung, Gerrit/Hartl, Korbinian, Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierungen und Datenschutzaudit, Zeitschrift für Datenschutz (ZD) 2014, 219-225.

Jäger, Bernd; Kraft, Reiner; Selzer, Annika; Waldmann, Ulrich, Die teilautomatisierte Verifizierung der getrennten Verarbeitung in der Cloud, Datenschutz und Datensicherheit (DuD) 40 (5), 2016, 305–309. DOI: 10.1007/s11623-016-0601-2.

Kühling, Jürgen, Buchner, Benedikt (Ed.), Datenschutz-Grundverordnung/BDSG Kommentar, 2. Auflage, München 2018.

Laue, Philipp/Nink, Judith/Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016.

Leimeister, Stefanie; Böhm, Markus; Riedl, Christoph; Krcmar, Helmut (Ed.), The Business Perspective of Cloud Computing: Actors, Roles and Value Networks. Proceedings of the 18th European Conference on Information Systems (ECIS 2010). Pretoria, South Africa.

Marston, Sean; Li, Zhi; Bandyopadhyay, Subhajyoti; Zhang, Juheng; Ghalsasi, Anand, Cloud Computing — The Business Perspective. In: Decision Support Systems 51 (1), 2011, 176–189.

Massonet, Philippe; Naqvi, Syed; Ponsard, Christophe; Latanicki, Joseph; Rochwerger, Benny; Villari, Massimo, A Monitoring and Audit Logging Architecture for Data Location Compliance in Feder-ated Cloud Infrastructures. In: Distributed Processing, Workshops and Phd Forum (IPDPSW) 2011. Anchorage, AK, USA, 1510–1517.

Mell, Peter; Grance, Timothy, The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. Gaithersburg, Montgomery, USA 2011.

Michener, William K.; Jones, Matthew B., Ecoinformatics: supporting ecology as a data-intensive science. In: Ecological and evolutionary informatics 27 (2), 2012, 85–93. DOI: 10.1016/j.tree.2011.11.016.

Möller, Knud, Lifecycle Models of Data-centric Systems and Domains: The Abstract Data Lifecycle Model. In: Semant. web 4 (1), 2013, 67–88. Online verfügbar unter http://dl.acm.org/citation.cfm?id=2595053.2595060.

NIST Cloud Computing Security Working Group, NIST Cloud Computing Security Reference Architecture. NIST. 2013. Online verfügbar unter https://csrc.nist.gov/publications/detail/sp/500-299/draft.

Ofner, Martin Hubert; Straub, Kevin; Otto, Boris; Oesterle, Hubert, Management of the master data lifecycle. A framework for analysis. In: Journal of Ent Info Management 26 (4), 2013, 472–491. DOI: 10.1108/JEIM-05-2013-0026.

Paal, Boris, Pauly, Daniel A. (Ed.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar, 2. Auflage, München 2018.

Pearce, Michael; Zeadally, Sherali; Hunt, Ray, Virtualization, in: ACM Comput. Surv. 45 (2), 2013, 1–39. DOI: 10.1145/2431211.2431216.

Pearson, Siani; Benameur, Azzedine, Privacy, Security and Trust Issues Arising from Cloud Computing. In: 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom). Indianapolis, IN, USA, 2010, 693–702.

Plath, Kai-Uwe (Ed.), DSGVO/BDSG, Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, 3. Auflage, Köln 2018.

Roßnagel, Alexander, Kommentierung der DSGVO, in: Simitis, Spiros/Hornung, Gerrit/Spiecker, Indra (Ed.), Datenschutzrecht – DSGVO mit BDSG, Baden-Baden 2019.

Roßnagel, Alexander, § 2 I. Anwendungsvorrang des Unionsrechts, in: ders. (Ed.), Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, Baden-Baden 2018, 41-54.

Roßnagel, Alexander, Datenschutzaudit - ein modernes Steuerungsinstrument, in: Hempel, Leon/Krasmann, Susanne/Bröcking, Ulrich (Ed.), Sichtbarkeitsregime, Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Wiesbaden 2011, 263-280.

Roßnagel, Alexander, Datenschutzaudit, Konzeption, Durchführung, gesetzliche Regelung, Braunschweig/Wiesbaden 2000.

Roßnagel, Alexander/Richter, Philipp/Nebel, Maxi, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, Zeitschrift für Datenschutz (ZD) 2015, 455-460.

Schneider, Stephan; Sunyaev, Ali, Cloud-Service-Zertifizierung. Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services, Berlin Heidelberg 2015.

Schwarze, Jürgen/Becker, Ulrich/Hatje, Armin/Schoo, Johann (Ed.), EU-Kommentar, 3. Auflage, Baden-Baden 2012 (zitiert: Autor, in: Schwarze u.a. 2012).

Singh, Saurabh; Jeong, Young-Sik; Park, Jong Hyuk, A survey on cloud computing security: Issues, threats, and solutions. In: Journal of Network and Computer Applications 75, 2016, 200–222. DOI: 10.1016/j.jnca.2016.09.002.

Sun, Da-Wei; Chang, Gui-Ran; Gao, Shang; Jin, Li-Zhong; Wang, Xing-Wei, Modeling a Dy-namic Data Replication Strategy to Increase System Availability in Cloud Computing Environments. In: J. Comput. Sci. Technol. 27 (2), 2012, 256–272. DOI: 10.1007/s11390-012-1221-4.

van Veenstra, Anne Fleur; van den Broek, Tijs, A Community-driven Open Data Lifecycle Model Based on Literature and Practice. In: Imed Boughzala, Marijn Janssen und Saïd Assar (Hg.): Case Studies in e-Government 2.0. Cham: Springer International Publishing, 2015, 183–198.

Villazón-Terrazas, Boris; Vilches-Blázquez, Luis. M.; Corcho, Oscar; Gómez-Pérez, Asunción, Methodological Guidelines for Publishing Government Linked Data. In: David Wood (Ed.): Linking Government Data. New York, NY: Springer New York, 2011, 27–49. Online abrufbar unter https://doi.org/10.1007/978-1-4614-1767-5_2.

Zhao, Liang; Sakr, Sherif; Liu, Anna; Bouguettaya, Athman, Cloud Data Management. Cham: Springer International Publishing, 2014.