European Cloud Service
Data Protection Certification

AUDITOR Certification Object

- Version 0.99c -

Status: 05/25/2021

Related AUDITOR publications:

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

Available online: www.auditor-cert.eu

Recommended Citation:

Roßnagel, A., Sunyaev, A., Lins, S., Maier-Reinhardt, N., & Teigeler, H. (2021). AUDITOR Certification Object – version 0.99c. Online available: www.auditor-cert.eu

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

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

Authors

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

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

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

UNIKASSEL VERSITÄT

provet

KIT Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES

Table of contents

List of abbreviations and acronyms

Art.	Article
BDSG n.v.	German Federal Data Protection Act (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 (letter)
No.	Number
Para.	Paragraph
R	Recital
TOM	Technical and organisational measures
w.m.o.	within the meaning of

Note on the gender-neutral wording:

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

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

The object of certification describes the data-protection-related 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 certificate's assertions. 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 (1) GDPR, may only use processors "providing sufficient guarantees" confirming that appropriate technical and organisational measures (TOMs) are implemented in such a way that processing meets 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 defines the cloud-specific object of certification from a technical point of view.

1. Derivation of 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 Section 39 of the Federal Data Protection Act (BDSG) fulfils the regulatory mandate of the Member States set out in Art. 43 (1) sentence 2 GDPR by delegating the accreditation of certification bodies to the German Accreditation Body and granting authorisation to issue data-protection-specific certificates as a certification body to the relevant data protection supervisory authority. Although the national legislator can also act in the area of certification without an explicit "opening clause" and implement its own regulations – provided that they do not contradict the regulations of the General Data Protection Regulation[1] – this is only the case as long as the national legislator merely clarifies vague legal concepts,[2] substantiates requirements for which greater detail is necessary, closes legal loopholes or supplements incomplete regulations.[3] Insofar as the General Data Protection Regulation is incomplete, needs to be supplemented or substantiated, co-regulation by the national legislator is therefore possible and necessary to make the application of the law practicable.[4] In principle, it is therefore also possible to regulate procedural issues relating to certification in accordance with Art. 42 GDPR in national law as a complement to the General Data Protection Regulation. However, such supplementary regulations have not yet been issued.

The General Data Protection Regulation no longer makes a distinction between auditing and certification, as was the case under German law before.[5] It does not focus on the certification of products or the auditing of data protection management systems.[6] Art. 42 (1) sentence 1 GDPR refers only to "data protection certification mechanisms" for the purpose of determining and demonstrating compliance of "processing operations". According to the wording of the Regulation, compliance with its requirements is therefore the audit standard and thus "legally implicit"[7] because the legal norms of the General Data Protection Regulation are binding in any case and breaches of obligations by controllers and processors are subject to very heavy fines. There are differing assessments of whether certification mechanisms can also include certification criteria that require a higher data protection standard than that laid down in the General Data Protection Regulation. In part, a higher standard is considered not to be possible

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.

due to the exhaustive nature of the Regulation. [8] But others consider that "extra" voluntary data protection in certification mechanisms is certainly possible,[9] provided that the additional requirements are in line with the objectives of the Regulation.[10] This view also appeared to be supported by the Data Protection Board (Board). Annex 2 of Guidelines 1/2018 on certification and identification of certification criteria[11] explained that certification mechanisms may not be misleading. They were assumed to be misleading, for example, if a certification mechanism bears the name "Privacy Gold Standard" but at the same time includes criteria that only reflect the minimum requirements of the General Data Protection Regulation.[12] In the accepted version 3.0 of the Guidelines 1/2018 on certification, [13] however, this view has been omitted. Whether it must be concluded from this that criteria catalogues for certification may only contain criteria that do not go beyond the statutory minimum requirements of the General Data Protection Regulation will not be discussed further here, as this does not play a role in determining the object of certification within the framework of AUDITOR certification.

Pursuant to Art. 42 (1) GDPR, the Member States, the supervisory authorities, the Board and the Commission are to encourage the establishment of data protection certification mechanisms and data protection seals and marks at the Union level in particular, 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, although the term processing is. According to Art. 4 (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 legal norm it can therefore be concluded, that any handling of personal data must be subject to an audit during certification.

1.1. Legal literature on the object of certification

Before the Board's guidelines for certification were presented, different views on the object of certification could be found in legal literature. On the basis of the wording of Art. 42 (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 put forward that certifications under Art. 42 (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 factors linked to infringements. Only processing operations could thus be the object of certification and not products as such.[18] According to this view, however, it should be possible for controllers or processors to certify all processing operations related to a product or service.[19] What

---

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, Version 3.0, June 2019.

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.

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

matters 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 prevent those requiring certification from only having sub-processes certified that are critical under data protection law to avoid the cost of certification of processing operations that are clearly not critical for compliance with data protection law.[21] This view was shared in some of the literature with the notion that the controller or processor could determine the object and scope of certification themselves.[22]

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

1.2. Board guidelines on the object of certification

Since June 2019, the guidelines on certification accepted by the Data Protection Board after public consultation have been available in version 3.0[25] and these include statements about 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. Depending on the object of certification, however, 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 in the organisational measures relating to processing operations, as well as the risks of the processing operation for the rights and freedoms of the data subjects.[28]

The Board's guidelines are also helpful in defining the object of certification, as the term processing operation term is placed in the context of the terms used in DIN EN ISO/IEC 17065, a standard which is important for certification of products and services. They clarify that processing operations or bundles of processing operations in the terminology of the Regulation result in 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 that form the object of certification must be clearly described. This includes specification of the data, processes and technical infrastructures.[30] Interfaces with other processes or services must also be considered and described. Even if only individual processing operations of a service are to be certified, for example, but a service consists of several processing operations, processing operations can only be excluded from the object of certification if they have no direct connection to the processing operations that are to be certified. In this case, too, the

[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, Version 3.0, June 2019.
[26] *European Data Protection Board*, Guidelines 1/2018, V. 3.0, marginal 52.
[27] *European Data Protection Board*, Guidelines 1/2018, V. 3.0, marginal 53 et seq.
[28] *European Data Protection Board*, Guidelines 1/2018, V. 3.0, marginal 56 et seq.
[29] *European Data Protection Board,* Guidelines 1/2018, V. 3.0, marginal 54.
[30] *European Data Protection Board*, Guidelines 1/2018, V. 3.0, marginal 58.

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 refers to "relevant products and services" as the object of certification, is[32] evident from the purpose of certification. Certification is ultimately intended to make it easier for controllers and processors to provide evidence of various audit and documentation obligations: certification must be considered "as an element" by which to demonstrate compliance with data protection law pursuant to Art. 24 (3) GDPR and with the requirements regarding privacy by design and privacy by default pursuant to Art. 25 (3) GDPR. It should also be taken into account when demonstrating sufficient technical and organisational security for processors pursuant to Art. 28 (5) GDPR and for the security of data processing pursuant to Art. 32 (3) GDPR. In addition, Art. 83 (2) lit. j GDPR stipulates 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 (2) lit. f, in conjunction with Art. 42 (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 not appropriate, as it would only be able to confirm a part of the technical and organisational measures of data processing by the controller or processor.[33] The way in which products and services are used by the controller or processor, rather than how they are offered by the manufacturer, is ultimately critical. Furthermore, in the case of a product certification the General Data Protection Regulation would have to address manufacturers and not a large number of users, but this is precisely what it does not do. 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 about 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 conformity with the requirements of the General Data Protection Regulation of the processing operations performed in products or services or with the help of (several) products and services. Such operations are within the sphere of influence of the controllers and processors and are largely defined by them; this explains, in turn, why they are the only addressees of certification mechanisms specified in Art. 42 (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, V. 3.0, marginal 59.
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” non-critical parts and certifying them is therefore not possible under the General Data Protection Regulation. Certification according to Art. 42 and Art. 43 GDPR does, after all, call for *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 (3) GDPR, allows for free determination of the object of certification, as the voluntary aspect refers exclusively to participation in the certification mechanism and selection of the specific data processing operation to be certified. The cloud provider cannot therefore 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 advisable for the cloud provider first to 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 for certification. It must also be clearly explained how the cloud user’s and cloud provider’s access options are structured in the data processing operations in question. These internal data processing steps and interfaces must be recorded in full.

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, a clear distinction between the responsibilities of cloud users and cloud providers, compliance with all principles of Art. 5 GDPR, 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, although 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 and 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 observed by all sub-processors at all levels. The cloud provider ultimately remains responsible to the cloud user for carrying out the processing. The cloud provider must therefore exercise due care when selecting sub-processors and may only cooperate with those who, in accordance with Article 28 (1) GDPR, provide “sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.” Sub-processors may, for their part, provide the appropriate safeguards required, 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.”

In summary, this means:

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.

When determining the object of certification, there are three components that cloud providers must consider as addressees of the AUDITOR certification mechanism: 1. personal data; 2. technical systems (infrastructure, hardware and software used to process the personal data) and 3. processes and procedures related to the processing operations. Thus, a data processing operation usually consists not only of technical and automated but also of non-technical organisational components, which are integrated into data protection concepts and 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 taken into account in their entirety. This means that interfaces of the cloud services to be certified with other services must also be considered in order to identify data flows from which data protection risks may arise. If the processing operations of a cloud service to be certified use platforms or infrastructures not owned by the provider or if the processor involves other sub-processors, the certificate may apply exclusively to the data processing operations which are within the responsibility of the processor concerned. 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 applicable to them and that it may use only sub-processors of this sort for the provision of its cloud service.

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

In order to determine the certification object, a complete data flow analysis should be conducted, including all the bodies involved in the processing of personal data. In particular, it should also be verified whether, in the course of the processing operations of the certification object, personal data is transferred outside the European Union or the European Economic Area or to international organisations. In addition, 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 on-demand 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 customise the performance parameters of utilised cloud services independently and almost immediately. In particular, this can be done automatically and without human interaction with the respective cloud providers. It is thus possible, for example, to increase or decrease the available 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 standard 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 allocated to different cloud users dynamically as needed. Cloud users are not always able to determine the exact location of the utilised resources. However, it is sometimes possible to narrow down the location approximately in terms of country, region or data centre.
- **Rapid elasticity.** The resources provided can be increased or shared flexibly and quickly, in some cases fully automatically, in order to match the resources to 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 measures, such as storage space, computing power or bandwidth. Usage-based billing (called 'pay-per-use') can therefore 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 available 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 can only adjust 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 and other services and tools supported by the cloud provider are used. In the same way as the Software as a Service model, the cloud user has no control over the underlying cloud infrastructure. On the other hand, users can manage applications which they have installed or carried out and may be able to adjust a limited number of settings in the relevant 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 software, such as operating systems or applications. The user is responsible for controlling the operating systems, databases and installed applications, and in some cases selected network resources such as firewalls, but not the underlying cloud infrastructure.

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).** However, only these three basic models will be discussed below.

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. As a matter of principle, the public cloud generally a selection of services for everyone (e.g. business processes, business practices, applications and infrastructures) at the same time over the Internet (multi-client capability) on the basis of usage-dependent payment. One of the most significant distinguishing features of a public cloud is that the cloud user cannot influence (either technically or contractually) which other parties use the cloud provider's cloud service. Thus, cloud users share the underlying infrastructure (without being aware of it or without knowing the extent and scope), which is, however, completely abstracted from the application layer. Adjusting to specific user requirements is usually only possible to a very limited extent or is 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 of the cloud service. One or more organisations of the community, third parties or a combination of the two 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 models (especially public and private cloud). The individual infrastructures remain as a unit but are connected by standard or proprietary technologies. This allows 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.** The term "virtual private cloud" was used for the first time 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 comprise a number of users (e.g. business divisions).[45] Access to the cloud service is provided by means of a Virtual Private Network (VPN). The cloud infrastructure is the property of the cloud provider. It is operated and managed by the cloud provider, while 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 shows examples of multi-cloud scenarios. The distinction between a multi-cloud and a hybrid cloud is problematic 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 provided solely by the Azure Cloud.

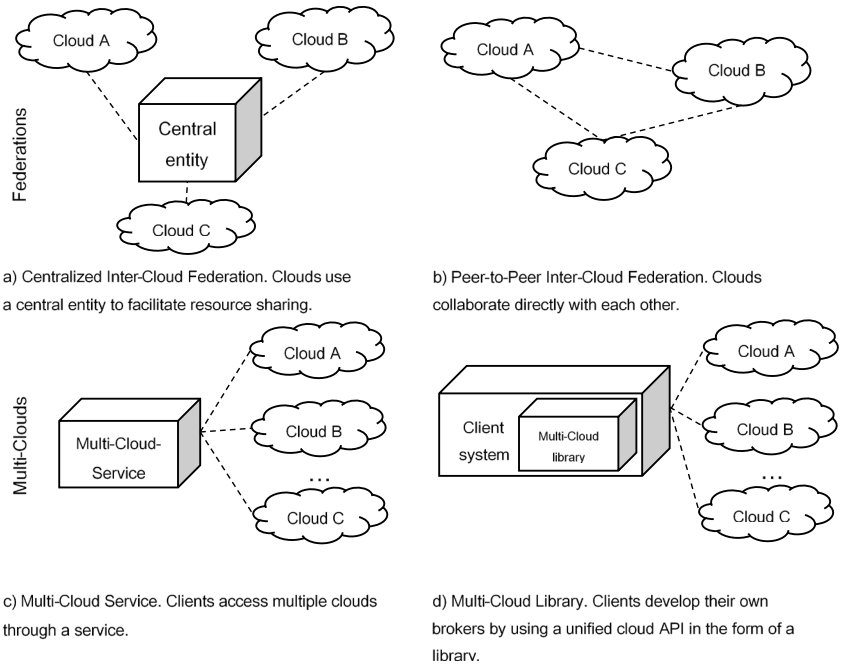


Figure 1. Examples of multi-clouds.[47]

2. Processing of personal data in the cloud

2.1. Definition of personal data

According to Art. 4 para. 1 GDPR, "personal data" refers to any information relating to an identified or identifiable natural person. A natural person is considered to be identifiable if they 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.

44 Amazon Web Services 2015.
45 *Dillon* et al. 2010.
46 *Grozev* und *Buyya* 2014.
47 *Grozev* und *Buyya* 2014.

2.2. Processing operations in cloud services

The following model is a graphical representation of a reference model for operations involving 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 in a series of operations.

In addition, individual consideration must be given to 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, because assignment is heavily dependent on the individual service model and the respective design of the processing agreement made with the cloud user. In particular, it should be noted that cloud providers are addressed by the AUDITOR Criteria Catalogue in two ways:

1) ***As the processors*** of data processing operations. Cloud providers can be both B2B and B2C providers. What is important is that they are involved as the processor of the data being processed in the cloud ("**content or application data**") and not as the controller, and they seek certification of the conformity of their data processing operations with data protection requirements. For B2B in particular, the content and application data will often be personal data of customers, employees, or other data subjects with whom the cloud user has a contractual relationship. However, content and application data may also be personal data of the cloud user.

2) ***As the controllers*** of data processing operations. Cloud providers are also addressed as the controllers of data processing operations, which are necessary to enter into and perform the contract for the provision of the cloud service with the cloud user. If the cloud service is offered in the B2C segment, the cloud user often represents the data subject, whose data are necessary to provide the cloud service, so that the cloud provider must fulfil its data protection obligations towards the cloud user (e.g. obligations to inform).

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

   Where the cloud user concludes a contract with the cloud provider for the provision and use of cloud services, the cloud provider will be obligated to process personal data foremost being subject to recording and retention obligations under commercial and tax law so that data processing for the fulfilment of legal obligations also falls within the scope of the AUDITOR certification.

   Although the cloud provider is generally free to choose the processing purpose and the matching legal basis under Art. 6 (1) subpara. 1 sent. 1 lit. a) to f) GDPR and Art. 5 (1) lit. b) in conjunction with Art. 6(4) GDPR does not have a strict purpose limitation but provides only for the reconcilability with the purpose, the AUDITOR certification exclusively examines the data processing of the cloud provider in its role as the controller, which is intrinsically linked to the contract between the cloud provider and the cloud user for the provision and use of the cloud service and the performance of the data processing. As part of the AUDITOR certification, only those data processing operations are considered, which are performed by the cloud provider in order to provide the cloud service to the cloud user so as to enable the use of the service and invoice the user accordingly for the service.

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

   To enable the cloud user to use the cloud service with the corresponding invoicing of the service to the user, the cloud provider must process additional personal data such as login/logout data for user accounts, IP addresses, the service modules used, and the extent of use. These data can be grouped under the term **"usage data"**.

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

When interpreting the following processing operation model, the following assumptions should be 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 operation 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 claim to completeness.
5. The model does not give any information about conformity to the GDPR. This is determined by the criteria stated in the AUDITOR Criteria Catalogue.

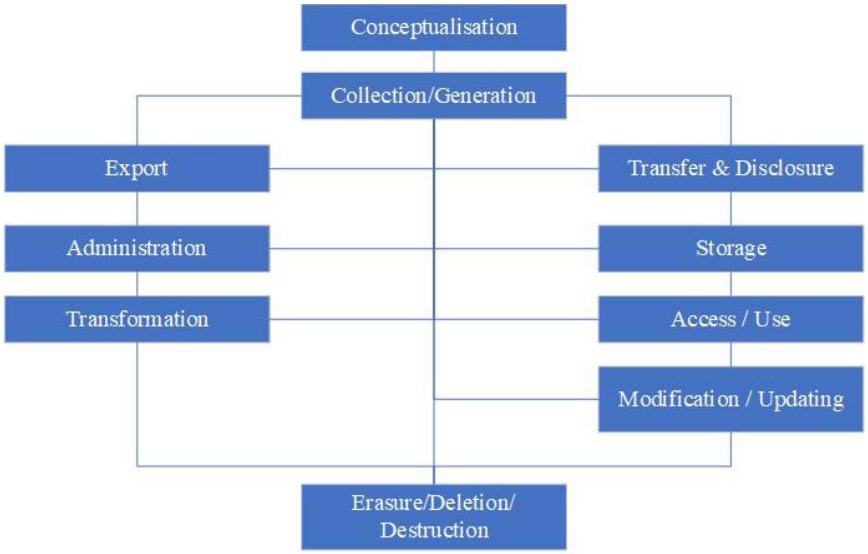


Figure 2. Processing operations model for (personal) data in the context of cloud services to support data flow analysis.

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 the 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	Purpose-related modification of data, particularly for security reasons.
Administration	Manual and automatic operations relating to the administration of data.
Export	(Complete) return of the data to the cloud user.
Erasure/Deletion/Destruction	Erasure of the data and, if necessary, destruction 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 very little or no 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).

This 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 subsequent definition of security measures to protect this data and the assignment of roles and responsibilities in data management, among other things. In addition, data requirements can also be specified with regard to quality requirements, for example, or the meta data needed. 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 the controller and **(2) master data 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.

Examples of content or application data:

- general personal data (name, date of birth, age, place of birth, address, email address, telephone number, etc.)
- identification numbers (social security number, tax 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 property ownership, land register entries, vehicle registration numbers, registration data, etc.)
- user data (orders, address data, account data, etc.)
- value judgments (school reports, examination certificates and work certificates, etc.)

Examples of master data:

- names
- addresses
- payment information such as bank account details
- phone numbers
- usernames and passwords for logging into the cloud service
- user-specific quality indicators, enabling monitoring or service provision

Examples of usage data:

- information about the beginning, end and scope of the respective service usage
- information about the telecommunications media used by the user
- log-in and log-out data for user accounts and IP addresses
- identification and authentication data for identifying the user and accessing the cloud service, such as usernames, IDs and e-mail addresses. In the case of multi-factor authentication, mobile numbers, fingerprints, the human voice or smart cards may be required
- technical data for service provision, such as the browser and device type used, operating system version, unique device identifiers, mobile network information, including phone number
- meta-data from the operation of the cloud service, such as log files that log data migration processes or store data locations. The personal reference of the data may be given directly or may result from a combination of various items of meta-data
- location data, if it is required for the use of the service. Various technologies are used to determine the location, such as IP addresses, GPS and other sensors, information about nearby devices, WLAN access points or mobile radio masts

[48] *Higgins* 2008.

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 reaches 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 techniques, 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 the available open data interfaces (e.g. databases or virtual machines offered) are sufficiently secure. In addition, Full-Stack and IaaS providers must monitor and secure transmission within the cloud infrastructure or between dispersed infrastructures. If data is 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 mechanism is not necessarily the responsibility of the cloud provider. It depends on the respective service model, 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 encrypting the communication, for example.	Secure interfaces for data reception or application integration.	Secure 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.
- **Data transmission to the cloud infrastructure via internal company networks.** When data is 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 is 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 cloud infrastructure (with multi-client capability).[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. for load balancing or redundant storage), 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 a 'cloud federation,' 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 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 disclosure of data to sub-processors who are indispensable

49 *Higgins* 2008.
50 *Bernard* 2007.
51 *Fernandes* et al. 2014.
52 *Jäger* et al. 2016.
53 *Jäger* et al. 2016.
54 *Massonet* et al. 2011.

for the service provision or disclosure 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 is disclosed. Particularly in the case of criminal prosecution, cloud providers may be required to support forensic data analysis through disclosure of user data.[55] Disclosure of data is not necessarily the responsibility of the cloud provider. It depends on the service model, 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 providing 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 advertising purposes for example.
- **Disclosure to the (security) bodies.** Under certain circumstances, data may be disclosed to law enforcement agencies or other government bodies.

2.2.4 Storage

Once data has been transmitted, a large number of processes may be initiated, some of which are considered below.

Preparation for data storage

Various processes can be performed in preparation for data storage. In accordance with the principle of data minimization, consideration should be given following collection or generation of data to whether the personal data have to be stored (in the long term).[56] Selecting which data to store reduces storage volume and cost and may minimise potential risks associated with storing sensitive data. Specification of volatile (e.g. DRAM) or non-volatile storage (e.g. HDD) could be made.

In addition, 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 is also a possibility in order to locate and use the data more effectively in future.[58] Measures can be also taken to ensure that stored data have a high degree of authenticity, reliability, usability, durability, accuracy and integrity.[59]

Implementation of data preparation operations is not necessarily the responsibility of the cloud provider. It depends on the respective service model, 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 the data and selects what will actually be stored on the basis of defined criteria that meet the requirements of the AUDITOR Criteria Catalogue or the instructions 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 that is necessary for storage, to determine the storage location, the data volume, the access rights or backup intervals for example.

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, various databases and storage technologies can be utilised. A variety of operations are also carried out to assist storage, including data partitioning. Implementation of data storage is not necessarily the responsibility of the cloud provider. It de-

[55] *Fernandes* et al. 2014.
[56] *Higgins* 2012.
[57] *Higgins* 2008; *Burton* und *Treloar* 2009; *Curtin* 2010.
[58] *Burton* und *Treloar* 2009)
[59] *Higgins* 2008, 2012.
[60] *Higgins* 2008.

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

Data backup

In order to guarantee the availability of stored data, a backup copy should be made. Backups are used to recover files if they have been tampered with or destroyed, etc. Redundant data storage is also particularly relevant in the context of the disaster recovery measures of a cloud service.[64] Implementation of a data backup is not necessarily the responsibility of the cloud provider. It depends on the respective service model, 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 is stored redundantly to increase availability and reliability. Backups are usually stored in different locations in the case of cloud services.
- **Creation of snapshots.** This involves a stored snapshot of a system or a database, for example. These support or enable data recovery. However, when snapshots are created in virtual machines, data stored in local or monitoring databases may be deleted accidentally under certain circumstances.[65]
- **Data recovery.** Corrupt data or data that has been tampered with or deleted can be recovered from backups or replicated data and then made available to the user again.

Data archiving

Data can also be archived. Data archives provide long-term storage of original versions of older data which are no longer relevant for day-to-day operation but are needed occasionally. Data archives are mostly indexed and equipped with a search function to retrieve data either in whole or in part. Implementation of data archiving is not necessarily the responsibility of the cloud provider. It depends on the respective service model, 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 suitability for archiving.** An ongoing process whereby data is 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.
- **Copying data from the database to the archive.** If the review of suitability for archiving identifies suitable data, it is moved to the archive and the storage space is freed up.
- **Accessing data in the archive.** Access to archived data may become necessary.
- **Deleting data from the archive.** Archiving over several years leads to a huge amount of data, which can be managed by deleting data according to defined retention periods.

61 *Jäger* et al. 2016.
62 *Zhao* et al. 2014.
63 *Sun* et al. 2012.
64 *Ofner* et al. 2013.
65 *Pearce* et al. 2013.

Migration of stored data

The concept of data migration is complex. 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 location of data storage.[67] Especially in the cloud computing environment, the storage and processing location of (personal) data is flexible and can usually be changed without much effort, on the grounds of load balancing, for example, or the availability of (redundant) data centres or flexible storage costs.[68] Suitable guidelines must therefore be established for migration of (personal) data within the cloud infrastructure. Implementation of data migration is not necessarily the responsibility of the cloud provider, depending on the respective service model, 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 data storage location.** In the context of load balancing, malfunctions or other reasons, a cloud service may change the location of the data and migrate it to another data centre.
- **A change of data format.** Changing the underlying technologies, software, hardware, or data models may require modification of the data formats. When data formats are changed, personal data may also be processed. For example, it may be necessary for personal data to be converted to a JSON format and stored in an XML format.

2.2.5 Access/use

A further central process is the read-access to the data. Here a distinction can be made between access by a cloud user to its own data and access to data by the cloud provider for further processing. To ensure secure access to personal data, adequate identity and access management systems and to guidelines are required.[69] Data access management is not necessarily the responsibility of the cloud provider. It depends on the respective service model, the design of the cloud service and the individual processing agreement made with the cloud user.

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 access verification, personal data is entered and compared with the data stored in the system.
- **Finding data.** In order to find the requested data, search operations can be performed, which may involve access to a large amount of personal data before the relevant data is found.
- **Read access by the cloud user.** The cloud user or an individual authorised by it initiates access to data, which is subsequently displayed or provided by the cloud service (e.g. 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 data 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 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 in the context of support activities, for example.
- **Read access by third parties.** With the consent of the cloud user, data may also be retrieved and used by third parties through defined interfaces in an application, for example.

2.2.6 Changes in the context of processing

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

---

66 *Higgins* 2008.
67 *Michener* und *Jones* 2012; *Alatorre* et al. 2014.
68 *Alatorre* et al. 2014.
69 *Higgins* 2008.
70 *Möller* 2013; *Higgins* 2008.

Significant data changes for cloud services include:

- **Changes by the cloud user.** The cloud user or an individual authorised by it changes or updates personal data, in the course of changing an address for example.
- **(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 make changes to data, in the context of support activities for example.
- **Changes by third parties.** Third parties may change or process data, insofar as there is a legal basis to do so, such as the consent of the data subject.

2.2.7 Transformation

In addition to modification of personal data in the context of the actual processing, it may also be transformed by secondary or support processes. This includes, for example, transformation processes such as filtering, harmonisation, synthesis, aggregation and enhancement. Transformations play a particularly important role in data protection. This includes, above all, encryption, pseudonymisation and anonymisation processes. Implementation of data transformations is not necessarily the responsibility of the cloud provider, depending on the respective service model, 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 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 process of compiling data and expressing it in the form of a summary.
- **Integration.** Merging of data from different sources into one data set.
- **Linkage.** Logical linkage of data creates a relationship between data from different sources.
- **Encryption.** The conversion of plain text by means of a key and an encryption algorithm into an encrypted text ('cipher text').
- **Anonymisation.** Anonymisation is the modification of personal data in such a way that it can no longer be ascribed to a specific or identifiable natural person, or this can be done only with a disproportionate amount of time, money and effort.
- **Pseudonymisation.** According to Art. 4 (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 is not attributed to an identified or identifiable natural person.

2.2.8 Administration

Processes for managing data can also be established. This includes, for example, quality assurance measures that are carried out (manually) and ensure high data quality,[71] and administrative activities based on instructions from the cloud user. Guidelines should be created to determine the administration of data.[72] Administrative operations are highly sensitive in the context of cloud services, since an administrator can, for example, cause data to be lost due to an error during data migration or while creating backups.[73] Administration of data is not necessarily the responsibility of the cloud provider, depending on the respective service model, the design of the cloud service and the individual processing agreement made with the cloud user.

- **Administration of data.** Cloud user support queries allow administrators of the cloud provider to manage data, including recovery of data and launching of virtual machines.
- **Review/tracking of data movements.** Automated or manual processes to review and analyse data traces can be performed to meet data locality requirements.

---

71 *van Veenstra* und *van den Broek* 2015; *Michener* und *Jones* 2012.
72 *Ofner* et al. 2013.
73 *Fernandes* et al. 2014.

- **Data verification.** Automated or manual processes can be performed to verify the accuracy of personal data; for example, verifying that the postal code entered corresponds to the location.
- **Identification of data anomalies.** Automated or manual administration operations can be performed to ensure data quality, 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 carried out in order to correct or delete data errors from databases, for example. These errors can result from incorrect, outdated or inconsistent data.

2.2.9 (Complete) export of data

At the end of the contractual period of the data processing or at the request of the cloud user, there are export operations that can be initiated to return the (complete) data. This is also known as backsourcing. Especially in the cloud computing environment, the portability of data is paramount for data return processes. Transmission of personal data in a structured, common and machine-readable format is therefore a requirement. Managing of the return of data is not necessarily the responsibility of the cloud provider. It depends on the respective service model, 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 it to the cloud user.

2.2.10 Erasure/deletion/destruction

The final step in data processing is the permanent deletion of personal data.[74] This can be done in particular at the request of the cloud user. With regard to cloud services, it should be noted that permanent and complete deletion requires special attention in the case of multi-client architecture, resource pooling, data redundancy and a distributed system architecture.[75] Physical destruction/deletion of storage media may be required. Erasure of data is not necessarily the responsibility of the cloud provider. It depends on the respective service model, 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. Simple techniques are usually used here, such as iterative description of the medium with an order of 0 and 1. Data clearing is only effective against simple, 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 is erased, including application data which is required for data processing.
- **Erasure of secondary data.** In addition, all secondary data of the cloud user is erased. This includes, in particular, backups, replications and meta-data.

[74] *Higgins* 2008; *Bernard* 2007.
[75] *Pearson* und *Benameur* 2010.

C. Scope of certification and responsibilities

For certification according to AUDITOR, the scope of certification and the field of application must be clearly defined. Identification and definition of the responsibilities of the cloud provider is important here, in particular to distinguish them from those of the cloud users and sub-processors.

1. Layered model for definition of responsibilities

1.1. Explanation of 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. On the basis of the cloud stack, the potential areas of influence for the cloud provider, the cloud user and any sub-processors can be determined. Table 3 is a schematic representation of the potential areas of influence. Depending on the architecture of the cloud service, variations may occur in practice. Moreover, a cloud service is not limited to a specific operational environment or layer. The layers can be spread out across all levels and, as a networked service structure, can be operated simultaneously by legally independent sub-processors. Thus, various parties or a combination of parties (e.g. cloud providers and sub-processors) may be simultaneously 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 usage of the application.
	User specifications	User specifications	User specifications	User-specific settings or configurations of applications used.
	Application	Application	Application	Available software solutions.
	Software security	Software security	Software security	Mechanisms for increasing the security of available applications.
	Administration and support for the software	Administration and support for the software	Administration and support for the software	Administration of the available software and receipt and handling of support enquiries 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 management and structuring of data.
	Platform security	Platform security	Platform security	Mechanisms for increasing the security of provided platforms.
	Administration and support for the platform	Administration and support for the platform	Administration and support for the platform	Administration of the available platform and receipt and handling of support enquiries from the cloud user.
	Virtual machines	Virtual machines	Virtual machines	Virtual representation of computer resources such as servers or CPUs.
Cloud provider	Virtualisation layer	Virtualisation layer	Virtualisation layer	Mechanisms for creating and managing virtual machines.
	Computation components	Computation components	Computation components	Components for conducting computations or processing of data in the cloud service.
	Storage	Storage	Storage	Mechanisms for storage of data.
	Network	Network	Network	Mechanisms for transfer of data.
	Infrastructure security	Infrastructure security	Infrastructure security	Mechanisms for increasing the security of available resources.
	Administration and support for the infrastructure	Administration and support for the infrastructure	Administration and support for the infrastructure	Administration of the available infrastructure and receipt and handling of support enquiries 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 cloud service.
	Connectivity and network connection			Physical connectivity of the data centre.
	Data centre security			Mechanisms for increasing the security of the data centre, including parties responsible for the premises, with security staff and physical security systems.

Table 3. Potential areas of influence according to the layer model.[76]

When using a SaaS service, the cloud user generally does not have the technical option to make alterations within the cloud service. The only option is for a cloud user to adjust certain configurations or settings in related cloud applications, such as turning certain features on or off or customising graphical user interfaces. 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 development, operation and administration of the software application and ensuring software security. The remaining cloud layers

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

are the responsibility of the SaaS Cloud provider (full-stack provider) or are outsourced to a sub-processor.

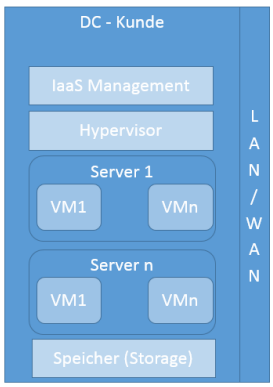
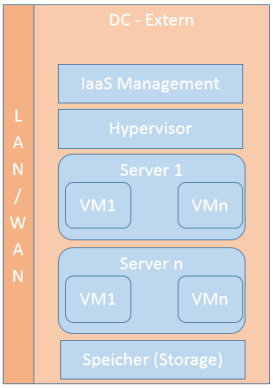
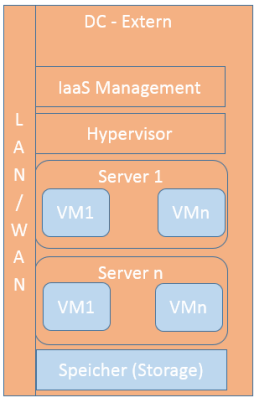
In the case of a PaaS service, cloud users run their own applications on a cloud platform provided. The cloud user is therefore responsible for creating and operating the applications. The cloud user must also deal with the security of the application in order to prevent cross-site scripting or software flaws, for example. The core business of the PaaS provider includes development, operation and administration of the platform (e.g. the systems and databases made available) and 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.

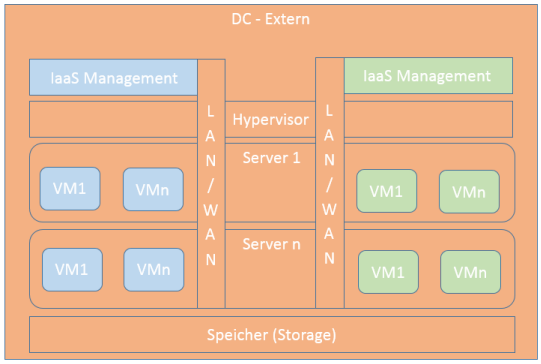
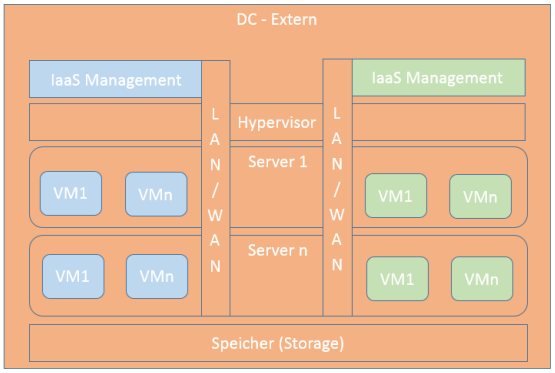
The cloud provider of an IaaS service is responsible for correct and secure virtualisation and provision of the necessary physical resources. A cloud user is responsible for the virtual machines leased and the applications, databases, operating systems and runtime environments used on them. In addition,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

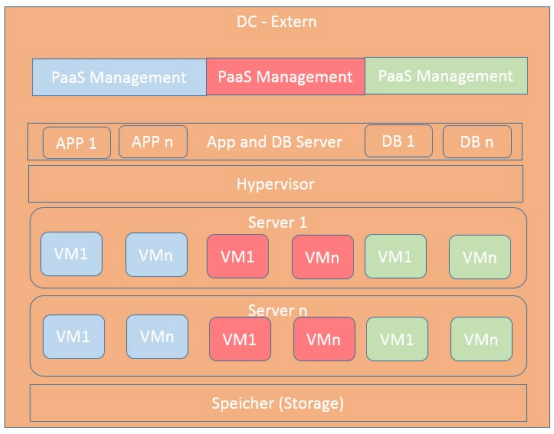
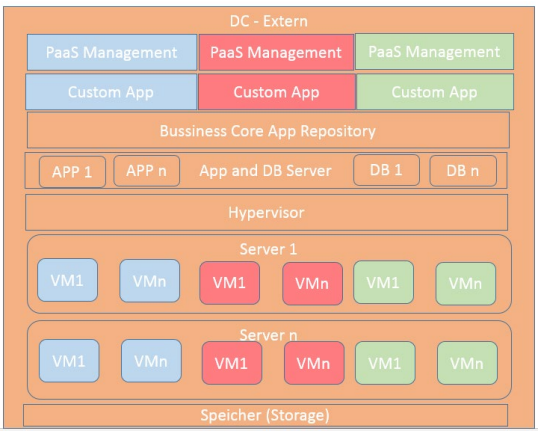
Depending on the specific design of the cloud service and the processing agreements made with cloud users, various responsibilities may arise. As far as further literature is concerned, reference is made to the NIST '*Cloud Security Reference Architecture*', which lists a detailed perspective of the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

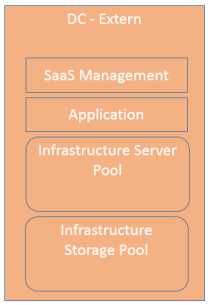
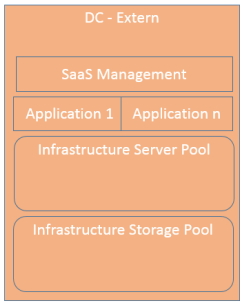
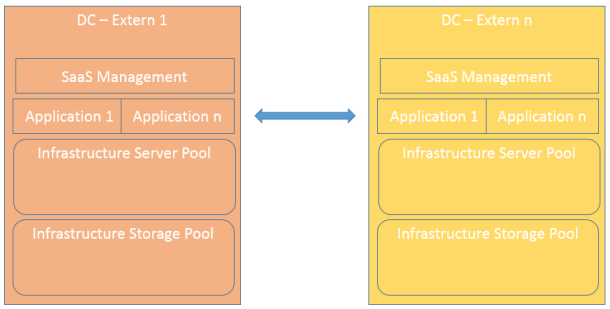
1.2. Illustrative examples

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

Private Cloud – On Premise	**Private Cloud – Externally Hosted**	**Private Cloud – Externally Managed**
In the case of "Private Cloud On Premise," it is assumed that the entire technical infrastructure can be controlled completely and immediately by the cloud user. 	In "Private Cloud Externally Hosted," the structure of the technical environment is made available 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. 	Over and above "Private Cloud Externally Hosted", the technical support of the system is handled by the cloud provider with direct access to both the system and the data. 
** Blue: Primarily the responsibility of the cloud user* *Orange: Primarily the responsibility of the cloud provider*		

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 specific client assignment for the dedicated use of a cloud user.	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.
	
** 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 Package	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 coordinated management.	The Public Cloud PaaS - Core Business App is a basic SaaS preliminary stage for application services, which can be customised to accommodate special needs via direct programming. These additional modules are provided as isolated applications in the Public SaaS model.
	
** 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.	The Public Cloud SaaS - Suite allows for a logical group of applications with multi-client capacity to be provided for public use.	The Public Cloud Multi SaaS - Suite allows for a logical group of applications with multi-client capacity to be provided for public use over several SaaS providers.
		
** Orange: Primarily the responsibility of the cloud provider* *Yellow: Primarily the responsibility of another cloud provider*		

2. Distribution of responsibilities between the cloud provider and the cloud user

Because the scope of the data protection certification under AUDITOR includes processing of personal data on behalf of the controller in accordance with Art. 28 GDPR, the AUDITOR Criteria Catalogue focuses on the legal data protection requirements that apply to the cloud provider in its role as processor. Data processing operations for which the cloud provider does not merely act under instruction but determines the purpose and means of processing personal data as the controller are considered in the context of the AUDITOR certification only where processing of personal data of the cloud user or other data subjects, such as employees of the cloud user, takes place to provide the cloud service and enable its use with appropriate billing, and where data processing serves to fulfil legal obligations applicable to the cloud provider.

It is not uncommon for cloud computing to result in responsibilities of the cloud provider and the cloud user existing in parallel. General guidelines on the distribution of responsibilities are difficult to formulate since it depends largely on the service models, the specific design and the individual processing agreements with the cloud users. It is therefore up to the cloud user and cloud provider to determine rules for distributing responsibilities.

The rules must reflect the actual distribution of possible areas of influence between the parties. The greater the cloud provider's opportunities to influence data processing, the more likely it will be viewed as the controller. According to Art. 4 (7) GDPR, the controller is the body that determines the purposes and means of data processing. The cloud provider is a processor if it carries out commissioned data processing in accordance with instructions and does not pursue its own purposes with the data that is processed. However, the cloud provider often has certain decision-making powers over the choice of technical and organisational means. Insofar as such means are suitable to achieve the purpose of processing and provided it informs the cloud user about them and the cloud user agrees to them, the cloud provider remains a processor.

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

3. Distribution of responsibilities between the cloud provider and the sub-processor

The cloud provider does not have to provide the full cloud service itself, but can use other subcontracted processors (sub-processors) to deliver services, provided that the cloud user agrees to this. In this case, individual sections or parts of the data processing can be delegated or outsourced to other processors, which results in a service chain.

However, outsourcing of the data processing to other sub-processors must not result in the provisions of the General Data Protection Regulation being disregarded in the service chain. Rather, the cloud provider as the main processor must ensure that the relevant provisions of the General Data Protection Regulation are observed by all sub-processors at all levels. The cloud provider has overall responsibility for execution of the instructions of the cloud user.

If the processing operations of a cloud service to be certified use platforms or infrastructures not owned by the provider or if the processor involves other sub-processors, the certificate may apply exclusively to the data processing operations which are within the area of responsibility of the respective processor. However, the processor must ensure that the third-party platforms, infrastructures and sub-processors used by it also comply with the data protection regulations applicable to them, and it is permitted to use only those that do so for the provision of its cloud service.

A cloud provider may therefore only select those sub-processors which, in accordance with Art.28 (1) GDPR, provide "*sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.*" Sub-processors can also provide the guarantees required in the form of a data protection certificate, for example, or by compliance with approved codes of conduct pursuant to Art. 40 GDPR. Section V of this Criteria Catalogue regulates subcontracted processing in particular.

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

Bibliography

Alatorre, Gabriel; Ayala, Richard; Chavda, Kavita; Gopisetty, Sandeep; Singh, Aameek, Data lifecycle management within a cloud computing environment. Publication number: US8918439 B2, 2014.

Amazon Web Services, AWS | Amazon Virtual Private Cloud (VPC) – Secure 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.), The new data protection regulations (in German: Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze), Baden-Baden 2018, 211-220.

Brink, Stefan, Wolff, Amadeus (Ed.), Data protection regulations (in German: BeckOK Datenschutzrecht), 24. Edition, Munich 2018.

Brühann, Ulf, Minimum standards or full harmonisation of data protection in the EC (in German: 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), European Journal of Business Law (EuZW) 2009, 639-644.

Burton, Adrian; Treloar, Andrew, Designing for Discovery and Re-Use. The 'ANDS Data Sharing 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.), GDPR (in German: DS-GVO, Datenschutz-Grundverordnung Kommentar), 2nd edition, Munich 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, available online at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en, last accessed: 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 and 32 of the Regulation 2016/679, Version for public consultation, 23.01.2019 available online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-0_en, last accessed: 01.03.2019.

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, available online at: https://www.european-privacy-seal.eu/EPS-en/Criteria, last accessed: 12.09.2018.

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? - Aims and contents of a data protection certificate (In German: Cui bono? – Ziele und Inhalte eines Datenschutz-Zertifikats), Data protection and data security (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 (Ed.): Managing Re-search Data. London: Facet Publishing 2012.

Hofmann, Johanna/Roßnagel, Alexander, Legal requirements for certifications under the GDPR (in German: Rechtliche Anforderungen an Zertifizierungen nach der DSGVO), in: Krcmar, Helmut/Eckert, Claudia/Roßnagel, Alexander/Sunyaev, Ali/Wiesche, Manuel (Eds.), Management of secure cloud services (in German: Management sicherer Cloud-Services, Entwicklung und Evaluation dynamischer Zertifikate), Wiesbaden 2018, 101-112.

Hornung, Gerrit/Hartl, Korbinian, Data protection through market incentives (in German: Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierungen und Datenschutzaudit), Journal for Data Protection (ZD) 2014, 219-225.

Jäger, Bernd; Kraft, Reiner; Selzer, Annika; Waldmann, Ulrich, The semi-automated verification of separate processing in the cloud (in German: Die teilautomatisierte Verifizierung der getrennten Verarbeitung in der Cloud), Data protection and data security (DuD) 40 (5), 2016, 305–309. DOI: 10.1007/s11623-016-0601-2.

Kühling, Jürgen, Buchner, Benedikt (Ed.), General Data Protection Regulation/BDSG Commentary (in German: Datenschutz-Grundverordnung/BDSG Kommentar), 2nd edition, Munich 2018.

Laue, Philipp/Nink, Judith/Kremer, Sascha, The new data protection law in operational practice (in German: 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 Federated 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. Available online at: http://dl.acm.org/citation.cfm?id=2595053.2595060.

NIST Cloud Computing Security Working Group, NIST Cloud Computing Security Reference Architecture. NIST. 2013. Available online at: 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.), General Data Protection Regulation German Federal Data Protection Act Commentary (in German: Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar), 2nd edition, Munich 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.), GDPR/BDSG (in German: DSGVO/BDSG, Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG), 3rd edition, Cologne 2018.

Roßnagel, Alexander, Commentary on the GDPR (in German: Kommentierung der DSGVO), in: Simitis, Spiros/Hornung, Gerrit/Spiecker, Indra (Ed.), Data protection law - DSGVO with BDSG (in German: Datenschutzrecht – DSGVO mit BDSG), Baden-Baden 2019.

Roßnagel, Alexander, § 2 I. Primacy of application of EU law (in German: § 2 I. Anwendungsvorrang des Unionsrechts), in: ders. (Ed.), The new data protection regulations (in German: Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze), Baden-Baden 2018, 41-54.

Roßnagel, Alexander, Data protection audit (in German: Datenschutzaudit - ein modernes Steuerungsinstrument), in: Hempel, Leon/Krasmann, Susanne/Bröcking, Ulrich (Ed.), Visibility regimes, surveillance, security and privacy in the 21st century (in German: Sichtbarkeitsregime, Überwachung, Sicherheit und Privatheit im 21. Jahrhundert), Wiesbaden 2011, 263-280.

Roßnagel, Alexander, Data protection audit, conception, implementation, legal regulation (in German: Datenschutzaudit, Konzeption, Durchführung, gesetzliche Regelung), Braunschweig/Wiesbaden 2000.

Roßnagel, Alexander/Richter, Philipp/Nebel, Maxi, What remains of European data protection law? (in German: Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO), Journal for Data Protection (ZD) 2015, 455-460.

Schneider, Stephan; Sunyaev, Ali, Cloud Service Certification (in German: 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 commentary (in German: EU-Kommentar), 3rd edition, Baden-Baden 2012 (cited: author, 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 Dynamic 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. Available online at: 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.