KuppingerCole

WHITEPAPER

by Dr. Karsten Kinast | December 2016

Cloud Computing and Data Protection

German cloud users of cloud service providers often have concerns whether the use of the cloud is acceptable from a data protection perspective, what they should look for in the contract with their cloud service provider and which measures they themselves should take in order to be compliant with the applicable data protection laws.

This Whitepaper shows most frequently asked questions about infrastructure as a service (IAAS) and provides answers according to official statements of German data protection authorities and other institutions with a strong expertise in this field.

Dr. Karsten Kinast
kk@kuppingercole.com

Commissioned by amazon web services

Content

FAQ 1 - Taking control

Cloud users of cloud services often wonder whether they really have to carry out an on-site audit.

Duty of the Cloud Service Provider (CSP): Implementation of technical and organizational measures

Section 9 of the German Federal Data Protection Act (BDSG) speaks of the implementation of technical and organizational measures required in order to be compliant with the law. The annex to section 9 BDSG defines such measures. Among these, the commissioned processing of personal data is named, specifying "the data is processed strictly in accordance with the instructions of the principal (job control)". So every cloud service provider ("CSP") must meet this obligation. Moreover, section 11 BDSG defines the obligations of other bodies collecting, processing or using personal data, to the extent that "the responsibility for compliance with the provisions of this Act and with other data protection provisions shall rest with the principal".

On-site audit as presumed duty for cloud users

Many cloud users believe that they have to carry out an on-site audit of the technical and organizational measures in order to comply with their legal obligations when using cloud services. Generally, as a cloud user you are the data controller and therefore, you are legally responsible for the data. That means, you have to fulfill several duties. *Please read also FAQ 2-9 for further details concerning your obligations as data controller.* The obligation to conduct an on-site audit of the technical and organizational measures of the CSP is often mentioned as a presumed duty. However, whether such a duty exists is doubtful.[1]

Duty of the cloud user

Within the relevant sections of the BDSG, there is no mention of a data protection "audit". Section 11 (5) BDSG states that "controls" should be undertaken. As the law does not clearly require an audit, there is no requirement for an on-site audit. According to the legal wording, "controls" should take place in order to fulfill the obligations of the data controller, i.e. the cloud user. There are different ways in which these control obligations could be met: On-Site audit, audit conducted by questionnaires, obtaining proof of third party certification.[2]

- □ Assure that controls take place with the appropriate frequency in order to determine that the technical and organizational measures are correctly implemented.

Control does not mean on-site audit

Even if the controller would prefer to conduct an on-site audit in order to meet the mentioned control obligations:

- □ you have to ask yourself as cloud user whether you are able to conduct an adequate on-site audit. Additionally, if your CSP permits on-site audits, do they provide this right to all customers? What implications does this have on the security of the premises?

Quality issues and liability related to a cloud user-conducted audit

Cloud users are most likely not to be experts in data protection and data security issues from an audit perspective; therefore, it is highly unlikely that they possess the same level of competence and professionalism as experts in these areas. An improperly conducted audit could expose the cloud user to liability.

[1] Arbeitsgruppe „Rechtsrahmen des Cloud Computing", Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, p. 8.
[2] Datenschutz und Datensicherheit, Annika Selzer, 2013, p. 215-219.

Conducting a high quality on-site audit on a frequent basis might just not be possible or feasible for the cloud user.[3] Bearing in mind that the quality of the audit depends on the expertise of the auditor and the frequency of the control, you have to ask yourself as a cloud user, if it is reasonable to do this yourself. Can you conduct frequent on-site audits, write reports and guarantee quality high enough to rule out self-liability while doing so. A high quality on-site audit or paper based audit via questionnaires can only be conducted by experts.

Third party certifications confirm state-of-the-art of security

From a practical point of view, this means that only certifications from third parties using internationally recognized standards provide a concrete alternative for cloud users to fulfill their control obligations.[4] A strong argument for this is that recognized standards are constantly evolving to match the developments in the state-of-the-art of security. On top of this, it is much easier for the CSP to provide a deep insight into the systems to a single qualified auditor than to provide this to many individuals. Therefore, it appears reasonable to rely on an auditor engaged by the CSP. It is important to recognize that you would not want everyone to have access to systems containing your data as this undermines the security of such systems. Therefore, not only the security of data is in best hands with experts but also the control of it.

As a result, independent certifications and attestations to widely accepted standards could be used in order to fulfil the control obligations[5] and reduce liability. For example:

- Cloud Computing Compliance Controls Catalog (C5)[6]
- ISO 27001[7]
- ISO 27018
- CSA STAR[8]
- TÜV Trust IT[9]
- There is also the possibility to attest compliance with the cloud Computing Compliance Control Catalogue by the BSI in form of a SOC 2-Report, provided by an independent accountancy auditor.[10]
- The Frauenhofer SIT suggests working with EuroCloud Germany_eco e.V. as an alternative to the previously mentioned standards. This has been developed as a “Seal of Approval” in coordination with the German BSI.[11]

– □ Review the extent to which the individual certification addresses data security and IT-risks in terms of your individual use of cloud computing.[12]

[3] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; “Orientierungshilfe – Cloud Computing“, p. 10.
[4] Datenschutz und Datensicherheit, Annika Selzer, 2013, p. 217.
[5] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; “Orientierungshilfe – Cloud Computing“, p. 40.
[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf, as consulted 22.09.2016
[7] Fraunhofer Institute for Secure Information Technology, „SIT Technical Reports on the Security of Cloud Storage Services“, p. 34; Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; “Orientierungshilfe – Cloud Computing“, p. 40.
[8] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/CloudZertifizierung/CloudZertifizierung_node.html, as consulted 22.09.2016.
[9] Ibid.
[10] Ibid.
[11] Fraunhofer Institute for Secure Information Technology, „SIT Technical Reports on the Security of Cloud Storage Services“, p. 35.
[12] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; “Orientierungshilfe – Cloud Computing“, p. 10.

Investigation of audit's outcome as sufficient control

As the legal wording only mentions "controls", the "investigation" of an audit conducted prior to a certification, is sufficient and is advisable in order to reduce the liability of the cloud user. This is due to the fact that the legal wording specifies neither the kinds of controls nor who should implement these controls on site. Furthermore, compared to a compulsory inspection or to a paper based audit via questionnaires, a certification by a third party can also be regarded as a high quality control providing the cloud user analyses the certification[13]. This is because the quality of the control itself is much more important than the presumed requirement to do this yourself.

Summarized audit report guarantees confidentiality

The cloud user could argue that the complete report of the audit by the third party has to be provided. However, as this would disclose all of the security measures, the CSP should be obligated to disclose only the proof of certifications by third parties[14], for example in form of executive summaries. As a result, the details of the security measure remain confidential. This is important, for example where the cloud user is a hospital and sensitive data such as health data is processed.

- □ Therefore, please check the results described in the executive summary of a third party audit report provided by the CSP.
- □ Check that the certifications cover risks associated with the kind of data being uploaded to the cloud.

It is commonly argued that the contract between the cloud user and the CSP should not state that the provision of certifications is the only possibility to fulfill the obligation to control.[15] In addition, it is recommended that the cloud user should review the scope of the certifications in terms of their own personal use and needs[16].

- □ Therefore, you are not required to conduct an on-site audit yourself, but you should request the results of the certifications and review if they meet your use of cloud computing.

On-site audit reduces level of security

In the age of cloud computing on-site audits conducted by individual cloud users could evolve into anachronistic form of audit-tourism.[17] Furthermore, there are details of security measures that are intentionally not disclosed by the CSP in order to keep the details of their security measures confidential to reduce risks. Therefore, an on-site audit is sometimes "just not possible"[18].

Is an event-triggered audit adequate and useful?

Another argument might be that at least when certain kinds of events occur, such as a data loss or a presumed data breach, the cloud user should conduct an on-site audit.

However, specifically if such an event occurs, you should seek advice from experts to analyze and handle the situation professionally. An existing third party certification would likely be too general to identify the possible security gaps leading to the event that occurred.

---

[13] Datenschutz und Datensicherheit, Annika Selzer, 2013, p. 218.
[14] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 12.
[15] Ibid. p. 11.
[16] Datenschutz und Datensicherheit, Annika Selzer, 2013, p. 217.
[17] Ibid. p. 219.
[18] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 10.

- □ Make contact with your service provider in these circumstances to find out whether the cause for the event can be determined faster and more safely without an audit.

Notwithstanding the foregoing, our consulting experience has shown that in most cases application errors and the cloud user's infrastructure are the cause for the situation in the first place. A professional CSP will be able to help you in terms of interfaces, access rights and general organizational issues. If more help is needed, we recommend that you get in contact with the relevant data protection authority. In any case, according to section 42a BDSG, there is an obligation to notify the relevant data protection authority if data breaches occur. Also, it is worth mentioning that if the source of error is on the CSP's side, the responsible data protection authority will be able to check the adequacy of the service provider's security measures irrespective of whether audit rights are agreed in the service contract or not.

FAQ 2 - Administration of the cloud services

Cloud users often ask what kind of legal requirements they have to fulfill in relation to the location of the data centers and their maintenance.

Liability risks in relation to the location of the cloud services and maintenance

The location of the cloud services, its maintenance and how this relates to the cloud user's liability is much discussed and often unclear to cloud users. This is due to the fact that further issues have to be taken in to consideration that depend on the location of the data processing and data maintenance.

Are there different legal requirements between the administration and maintenance within and outside of the EEA/Switzerland?

The German legal wording, section 4b BDSG, states that "particular consideration shall be given to the nature of the data, the purpose, the duration of the proposed processing operation, the country of origin, the recipient country and the legal norms, professional rules and securities measures which apply to the recipient" in order to guarantee adequate data protection. Looking at European requirements, for example at the European Directive 95/46/EC[19] and at the European Regulation 2016/679[20], better known as the General Data Protection Regulation (GDPR), data processors located within the EEA/Switzerland are not permitted to transfer personal data to a country outside of the EEA/Switzerland unless the recipient is able to guarantee the same level of data protection. Therefore, it is necessary to distinguish whether the data is processed - the services are administered or even if they are only mirrored- within or outside of the EEA/Switzerland. For data processing within the EEA/Switzerland, German cloud user should require a data processing agreement according to section 11 BDSG to be signed. According to section 11 (5) BDSG this duty exists "if other bodies are commissioned to carry out the inspection or the possibility of personal data being accessed cannot be excluded" which for CSPs is usually the case.

If the data is processed outside of the EEA/Switzerland, in order to make sure that the same level of data protection is guaranteed by your service provider, for example by the implementation of Standard Contractual Clauses[21]. According to the Standard Contractual Clauses "any person acting under the authority of the data controller,

[19] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, as consulted 22.09.2016.
[20] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en, as consulted 22.09.2016.
[21] Ibid.

including a processor, must not process the data except on instructions from the controller"[22]. Once the Standard Contractual Clauses are implemented, the obligation to act as agreed in the prime contract between the cloud user and CSP is passed on to sub-contractors[23] and the liability will be handed over as well. *Please see FAQ 9 for further information about sub-contractors.* As a result:

- □ First of all, whenever third party providers or sub-contractors as CSPs are used, you must get confirmation of the location of your data[24], including information covering the mirroring, storage and maintenance of the data.
- □ In the case where the data originated in Germany and is processed within the EEA/Switzerland a Data Processing Contract according to section 11 BDSG shall be signed.
- □ Where the data is transferred outside of the EEA/Switzerland, you should implement the unmodified Standard Contractual Clauses released by the European Commission[25], sign Binding Corporate Rules or join the EU-U.S. Privacy Shield. This is necessary to ensure that you have the required contracts in place and have information about the transfer of your data needed to meet your legal obligations.

FAQ 3 - Legal intercept

For cloud users it is important to know whether the data stored in the cloud can be intercepted based on any legal framework.

Possible access by authorities

Often cloud users wonder if authorities could legally be able to get access to their data stored in the cloud. This question is frequently asked with regard to US authorities and whether they have access to this data. However, this question not only concerns data stored in the US but also, in individual cases, may affect the data stored within the EEA/Switzerland where the mirroring and/or access is/can be carried out from the USA.

Technical possibilities

In case the respective authority requests access and a judicial order is granted, the CSP, due to technical restrictions, may only able to provide access to bulk data and not to the specific data requested. This may make it impossible to fulfill what is usually a more specific judicial order/certain individual judicial orders. Also, some of the judicial orders may turn out to be unlawful according to a German legal understanding. Then, access taken upon these orders are considered in German Law to be unauthorized. If the cloud service model is Software as a Service (SaaS), it may be possible for the CSP to allow access only to specific data.

Access to be granted only if specific judicial order is given?

Where the data is stored within the EEA/Switzerland, the local and European data protection laws apply and the service providers have to act according to these laws. Nevertheless, other countries outside the EEA/Switzerland may have implemented legal frameworks, which provide the authorities with the permission to intercept data under specific circumstances. Looking for example at the US, the failed renewal of certain provisions of the USA Patriot

[22] Standard Contractual Clauses, Appendix 2.
[23] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 15.
[24] Ibid p. 14.
[25] Ibid p. 16.

Act[26] led to the introduction of the USA Freedom Act[27]. Both the USA Freedom Act as well as the Patriot Act state that the government can make requests to access data from the private sector related to foreign intelligence, counterterrorism, and criminal investigations. However, the USA Freedom Act tries to strengthen the judicial influence on these requests in order to prevent the "bulk" collection of records by requiring enhanced specificity in these requests. Nevertheless, it cannot be said, that US service providers act outside the law or that they do not protect the data of their cloud users against unauthorized access requests by the authorities without a judicial order. Most recently, the two prominent cases where both companies denied access requests got a lot of publicity as they acted according to international standards and in order to protect their customers' data against unauthorized access.

Cloud user's duty: encryption

Due to the practical and legal possibility of being subject to unauthorized access, CSPs no doubt understand the unease that these practices may cause in their cloud users. Section 9 BDSG and its annex define technical and organizational measures, which should be implemented so that no unauthorized access can occur. In this context "the use of the latest encryption procedures" in order to prevent access without authorization is mentioned as a way to ensure compliance with the law. *Please see FAQ 4 for further information about encryption.* Moreover, the US law states that the respective authorities are able to get access to data with low judicial influence[28], whereas the German law only recognizes the request to access the data based on a specific judicial order. As a result:

- □ Please verify that the CSP only responses to legitimate access requests of the responsible authorities.
- □ As it cannot be ruled out that the authorities in some countries may get access to the data transmitted into the cloud, the cloud user should consider encrypting confidential data so as to prevent unauthorized access[29].
- □ It is recommended to encrypt the respective data on the cloud user system before uploading it into the cloud by using a key unknown to the service provider[30].
- □ On top of this, please make sure, that the encryption method used is state-of-art of security.[31]
- □ The cloud user should be aware that a vulnerability in the cloud user software and configuration poses a risk[32].

FAQ 4 - Liability

Cloud users often wonder who is responsible for their data and its protection.

Definition of each party's liability

When you decide to use cloud services, you may consider the extent to which each of the parties (you and the CSP) is responsible for ensuring the adequate protection of the data stored in the cloud. The scope of the responsibility of each party should be well defined where personal information will be processed and various data categories are

[26] https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf, as consulted 22.09.2016.
[27] https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf, as consulted 22.09.2016.
[28] Ibid.
[29] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 12; Fraunhofer Institute for Secure Information Technology, „SIT Technical Reports on the Security of Cloud Storage Services", p. 53-54; German Federal Ministry for Economy and Technology, „Anbieterwechsel im Cloud Computing; Wege zur Steigerung von Akzeptanz und Vertrauen", p. 16.
[30] Fraunhofer Institute for Secure Information Technology, „SIT Technical Reports on the Security of Cloud Storage Services", p. 44.
[31] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 12.
[32] Fraunhofer Institute for Secure Information Technology, „SIT Technical Reports on the Security of Cloud Storage Services", p. 53.

affected. Both parties, the cloud user and the CSP, shall identify their own scope of responsibility according to the BDSG.

Identification of your role as controller

From a data protection perspective, the cloud user, as controller, is responsible for the personal data stored in the cloud. The controller is the "person or body collecting, processing or using personal data on its own behalf or commissioning others to do the same"[33]. When a contract for cloud services is signed, the cloud user commissions the CSP to process data on its behalf (*please read FAQ 2 and FAQ 9 for further information on commissioned data processing)*. The CSP is the person or body "commissioned to collect, process or use personal data"[34] (i.e., the processor). Since the cloud user is responsible for the data even while being processed in the cloud, the cloud user must ensure that the CSP has adequate safeguards in place to protect of personal data[35].

- □ Prior to storing data in the cloud, you should make sure that you comply with the relevant data protection requirements related to your role as a controller ("verantwortliche Stelle")[36].

That means in practice:

- □ Make sure that personal data has been obtained lawfully, either with the individual's consent or according to any applicable legal provisions (such as tax or labor law related regulations), and that individuals are informed about the further storage of their data in the cloud[37] . Also, make sure that the personal data collected is proportional and the personal data is used only for the purpose(s) for which it was collected. *Please read FAQ 5 for further details about deletion.*
- □ Make sure that you choose a CSP that ensures safeguards for the protection of personal data, including the implementation of adequate technical and organizational measures according to section 9 BDSG. *Please see FAQ 1 for further information about the necessary contract*.

Cloud strategy

In the context of cloud computing for business purposes, personal and confidential data may be stored in the cloud. Therefore, a "cloud strategy" should be defined in advance. In this strategy, your own IT-structure plays an essential role. You should consider whether your current systems are compatible with the use of cloud services, and whether this involves a risk for your company or for the individuals whose data is stored in the cloud. Also, organizational aspects such as access rights, retention periods and authentication methods need to be taken into consideration by the cloud user[38].

- □ Make sure that you comply with the principles of availability (timeframe in which data is available), confidentiality (no unauthorized disclosure of data) and integrity (no unauthorized changes or manipulation of data).

[33] Section 3 (7) BDSG; Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, p. 20.
[34] Section 11 (1) BDSG.
[35] Section 11 BDSG; Fraunhofer Institute for Secure Information Technology, „ SIT Technical Reports on the Security of Cloud Storage Services", p. 30-31; Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, p. 8, 12.
[36] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, p. 7-8.
[37] Section 4 (1), (2) BDSG.
[38] German Federal Office for Security on Information Technology, "Sicherheitsempfehlungen für Cloud Computing Anbieter", p. 19.

Adequate IT-infrastructure to minimize the impact of data breaches

The implementation of adequate technical and organizational measures may help the cloud user minimize the impact of a data breach or a data loss. The CSP is not responsible for the cloud user's technical and organisational measures or the cloud user's IT-infrastructure. In the event of a data breach, the cloud user must be able to recover data, for example through back-ups. The CSP may not guarantee the availability of the data stored where technical problems or data breaches occur on the cloud user's side. In addition to this, the cloud user must to check which data is backed-up and ensure that these back-ups take place periodically.

- □ Make sure that your data remains available also in case of data breach or if technical problems arise.

Cloud user: responsible for the use of the cloud

The cloud user is also responsible for the way in which the cloud is used. The CSP might not have access to or control over the data stored by the cloud user, therefore the CSP cannot assume responsibility for the content that the cloud user stores[39]. If the cloud services are used to store data related to criminal activities (fraud, money laundering, pornography, intellectual property violations, etc.), the cloud user may be held liable and this could result in the immediate termination of the contract by the CSP without notice. The cloud user is also responsible for ensuring that additional safeguards and technical measures are in place to protect sensitive data. *Please read FAQ 6 for further details about contract termination*.

- □ Make sure that the stored data does not involve a risk for the rights and freedoms of individuals and ensure that the data is uploaded lawfully and does not violate any applicable laws or regulations.

Why should data be encrypted?

Encryption is an essential aspect of technical security measures. The cloud user should encrypt data before and while this data is stored in the cloud[40]. This way, even if the CSP suffers a data breach, the cloud user's data would not be misused[41] and the damages caused to individuals might be reduced considerably. *Please read FAQ 3 for further details about the relevance of encryption.*

- □ Make sure that your own IT-infrastructure is adequate for your data processing activities and implement encryption.
- □ Ensure that security or back-up copies are made at your own premises in order to minimize risks.

Written agreements for commissioned data processing

There must be a written agreement for commissioning of the data processing to a CSP. This will ensure that the cloud user maintains the control over the data and that the CSP stores, processes or deletes data only under the instructions of the cloud user and not for any other purposes. *Please read FAQ 5 for further details about data deletion. Also, please read FAQ 2 and FAQ 9 for further details about commissioned data processing.* The agreement would set out the relevant technical and organizational requirements that the CSP will implement and include terms

[39] OLG Düsseldorf, Sentence from 27.04.2010 – I-20 U 166/09 ("Rapidshare").
[40] Fraunhofer Institute for secure Information Technology, „ SIT Technical Reports on the Security of Cloud Storage Services", p. 44; Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 13-14.
[41] German Federal Ministry for Economy and Technology, „Anbieterwechsel im Cloud Computing; Wege zur Steigerung von Akzeptanz und Vertrauen", p. 16.

regarding the support the CSP would provide to the cloud user in cases where the individuals exercise their rights to access, delete or correct the personal data held about them[42].

Role of certifications

Certifications possessed by a CSP may be a useful factor that can help to choose an adequate cloud provider. However, certifications do not exempt the cloud user from meeting its own data protection obligations. *Please read FAQ 1 for further details about certifications of CSPs*.

- □ The agreement with the CSP should describe the CSP's obligations relating to data protection and data security, as well as the scope of the processing.

International data transfer agreement

The use of cloud services may involve the transfer of the data to countries outside the EU. Where the transfer will be to a country that has not been declared by the EU as providing an adequate level of protection for personal data, you must ensure that the necessary data transfer agreements are in place. *Please read FAQ 2 and FAQ 9 for further details about the management of the cloud services and about international data transfers respectively*.

FAQ 5 - Data delete

It is important for cloud users to know who is responsible for the deletion of data stored in the cloud.

Implementation of data deletion and retention concepts

The use of cloud services implies the upload of different types of data (financial, personal or payroll data, employee data, personal pictures or videos, etc.). It is important to know which categories of data are stored in the cloud and when each data category should be deleted in order to minimize the risk of loss or misuse. Therefore, it is necessary to establish a data deletion concept. In addition, the retention periods specified in certain legal provisions shall be taken into consideration.

- □ In order to comply with data deletion and data retention obligations, you should consider implementing a data management strategy including a data retention policy.

What is meant by deletion?

The BDSG defines deletion as the process by which data is made unrecognizable[43]. Unrecognizable means that data cannot be retrieved anymore. There are several methods to make data unrecognizable such as the destruction or overwriting of devices where it is stored or by the deletion of links that give access to the data. Where only the links are removed that data may still exist on the media and could be recovered by forensic tools when the media is discarded.

- □ Data shall be deleted in such a way that a reconstruction of the information is not possible[44], see section 3 (4) No. 5 BDSG ("defacing").

[42] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, p. 9; Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 13.
[43] Section 3 (4) Cif. 5 BDSG.
[44] German Federal Office for Security on Information Technology, "M2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten".

Maximum retention periods

In addition, the maximum retention periods shall be taken into consideration depending on the categories of the data stored and the applicable legislation. In Germany, different laws set specific retention periods. In these cases, there is a legal obligation to retain data, so that a deletion is prohibited during a given period.

- □ Define specific retention periods for the data stored in the cloud.
- □ Define a data deletion policy adapted to your processing activities.
- □ Make sure you comply with the deletion and retention periods established by specific laws.

Deletion obligation for cloud user

The cloud user as data controller, is responsible for the deletion (= "defacing") of the data stored in the cloud[45]. This means that should it be ensured that data is deleted according to the relevant deletion policies, but also that the CSP deletes data according to the contractual provisions once the data is deleted from the cloud and/or the cloud contract has been terminated, *for the latter please see FAQ 6.* Moreover, the cloud user needs to ensure that personal data is not stored longer than necessary for the purposes for which this data was collected[46].

- □ Delete data from the cloud and all devices when it is no longer relevant for the purposes for which this data was collected.

Contractual provisions on data deletion

The agreement between the cloud user and the CSP shall include a provision on data deletion, in which the deletion terms are addressed[47]. This could be also specified in the terms of service or in an annex to the agreement. There are no specific certifications for data deletion, as there are for IT-Security aspects.

- □ Make sure that your agreement with the CSP includes a provision about data deletion, or this is regulated in the terms of service or an additional annex.
- □ Implement deletion methods and processes that are required for your IT-infrastructure.

Approved deletion method by the BSI

From a data protection perspective, the German Federal Office for Security on Information Technology (BSI) considers that data deletion has taken place, whenever any of the methods and processes described in the IT Security Catalogue (IT Grundschutz-Katalog) have been used[48].

- □ Check what type of deletion processes and methods are implemented by your CSP.

[45] Section 35 (2), (3) BDSG.
[46] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, p. 11-12.
[47] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, p. 12-13.
[48] For detailed information about deletion methods and processes, please consult the documents from the German Federal Office for Information Technology: "M2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten" and „M.2.433 Überblick über Methoden zur Löschung und Vernichtung von Daten".

Technical deletion aspect

Due to the complex IT-Infrastructure of CSPs, an immediate deletion of data may not be technically possible. The technical deletion, erasure or destruction of data may occur at a later point, depending on factors like the deletion processes implemented by the CSP. The CSP may have such an IT- infrastructure that can block access to data[49] until effective deletion takes place. Data deletion will then take place as soon as it is technically possible. This is a permitted approach as an earlier action may not be realized.

- □ You shall not expect an immediate deletion of data by the CSP, due to the complexity of the cloud infrastructure. CSPs shall be given a reasonable period of time to delete data from its devices and IT-infrastructure after the data has been deleted from the cloud and/or the cloud contract has been terminated, *please see FAQ 6*.
- □ Check that your CSP implements adequate technical and organizational security measures in order to protect your data from unauthorized access until the data deletion is definite.

FAQ 6 - Termination of contract

Cloud user often ask what happens with the data upon termination of the cloud services.

Reasons for a contract termination

The contract for cloud services may terminate for many different reasons, some of these reasons may be anticipated in the service agreement while some may be due to unpredictable circumstances. At this point, it is important to have a contractual provision that covers the period of time following the termination of the contract, as you may not be able to use the agreed cloud services during that period.

- □ Make sure that your cloud service agreement includes a clause about termination conditions.

The cloud service agreement may be terminated in one of the following cases:

- If the duration of the contract expires, or
- if the cloud user decides to stop using the cloud services provided by the CSP, or
- if the CSP ceases unilaterally to provide these services either due to “convenience” or because the cloud user has breached the terms of use set by the CSP, for example by using the cloud services for illegal purposes, or if the cloud user has not paid for the provided services[50].

- □ Make sure that the agreement also specifies the cases in which the agreement shall be deemed to be terminated[51].

[49] Section 35 (3) S. 3 BDSG; Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, p. 11.
[50] Termination „aus wichtigem Grund“, according to Section 543 (1) BGB for Rental Agreement and section 314 (1) BGB for agreements in general.
[51] Section 11 (2), (10) BDSG.

Deletion periods after the termination of the contract

In all of the above cases, the cloud user shall delete the stored data according to the terms of the agreement. In case of an ordinary termination of the agreement, the CSP will usually give the cloud user a reasonable period of time to delete their data stored in the cloud or to transfer it back to the cloud user's database. Often, the cloud user may only terminate the contract after they have deleted/transferred their data. When the CSP terminates the contract, the cloud user may also be given a period of time in order to comply with its obligations regarding deletion of data from the cloud. This will facilitate cloud users to delete their data from the cloud securely and to minimize the risk of a data loss or misuse. *Please read FAQ 5 for further details about deletion of data*.

- □ If you decide to stop using the cloud services, make sure that you delete your data from these services.
- □ Contact your CSP if you need and extension in the time needed to delete your data from the cloud.
- □ Assure that period granted for deleting your data is sufficient if the CSP terminates the contract.

After the cloud user has deleted the data from the cloud, the CSP shall ensure that no further data remains. The technical processes for the deletion of personal data take place within the CSP infrastructure. Until the data is definitively erased through its normal methods and processes, the CSP may block the access to that stored data through adequate technical measures. *Please read FAQ 5 for further details about deletion of data*.

FAQ 7 - Employees and data protection

Cloud users often query the role of non-disclosure agreements (NDA) and training for employees of the CSP.

How to ensure that employees handle personal data lawfully

Cloud users often ask if the employees of the CSP are trained in data protection and are committed to confidentiality. If this is the case, it provides assurance that CSP employees handle personal data according to the legal requirements and know how to act in the event of emergency, such as data breaches.

Implementation of a commitment to confidentiality

According to section 5 BDSG, persons who deal with personal data shall not process it without the appropriate authorization. Moreover, this section sets an obligation to undertake a commitment to confidentiality of anyone who processes personal data. The CSP, upon the entry into the contract with the cloud user, shall ensure that the data obtained will remain confidential and will not be disclosed to third parties.

However, by using a written and signed statement or introducing a clause in their employment contract the CSP will be able to prove compliance with this obligation[52] . The commitment to confidentiality implies that employees are informed about their obligations regarding the processing of personal data according to the BDSG[53].

As the cloud user is responsible for the data, he/she may demand evidence from the CSP that the confidentiality obligation has been met.

- □ Make sure that the CSP commits all employees to confidentiality.

[52] German Federal Commissioner for Data Protection and Freedom of Information (BfDI), "Datengeheimnis", http://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/Was_ist_Datenschutz/Artikel/Datengeheimnis.html, as consulted 21.09.2016; German Federal Office for Security on Information Technology, "Cloud Computing Controls Catalogue (C5) – Criteria to assess the information security of Cloud Services", 02/2016, p. 31.

[53] German Federal Office for Security on Information Technology, "Sicherheitsempfehlungen für Cloud Computing Anbieter, p. 64.

Raising awareness through data protection training

Moreover, persons that handle data should be aware of responsibilities inherent to these tasks, as well as the importance of IT-security and data protection in daily business. This could be achieved by awareness trainings. According to the BDSG, such training is obligatory in cases where a Data Protection Officer (DPO) is appointed[54]. *Please read FAQ 8 for further details about the role of a DPO*.

Additionally, the German Federal Office for Security on Information Technology requires CSPs to train employees on existing policies and instructions, roles, responsibilities and threats, as well as on the appropriate handling of data[55].

- □ Make sure that your CSP conducts regular data protection training for at least those employees who may under any circumstances have access to personal data, e.g. systems administration.

In any case, the cloud user shall also ensure that his/her own employees are aware of data protection issues. Therefore, the cloud user should ensure that all people who process data within their organization undertake data protection training and make commitments to confidentiality.

- □ Also, raise awareness on data protection issues within your own company.

FAQ 8 - Contact to Data Protection Officer

For cloud users it is important to know how to receive information about data protection at the CSP.

Obligation to appoint a Data Protection Officer (DPO)

CSP often receive enquires from cloud users, employees or third parties regarding the processing of personal data and other related questions. The CSP shall identify the person responsible to address these issues.

In order to ensure that data protection enquiries are correctly addressed, the CSP shall designate a point of contact specialized in data protection. For many German organizations, this is even obligatory if more than nine employees process personal data as a DPO will have to be appointed if more than nine employees process personal data.

With the upcoming GDPR this will also be obligatory in specific cases, so that in such circumstances not only German but also other EU-based organizations may be subject to the obligation to appoint a DPO.

Same obligation for data processing outside of Germany?

Where the data processing takes place outside of Germany, the CSP is not the “responsible body” according to section 1 (5) sentence 2 BDSG, and therefore, the requirement to appoint a DPO in this case is not given[56] unless the cloud service contract declares German law to be applicable.

[54] Section 4g (1) No. 2 BDSG.
[55] German Federal Office for Security on Information Technology, “Cloud Computing Controls Catalogue (C5) – Criteria to assess the information security of Cloud Services”, 02/2016, p. 31.
[56] Cf. Teager/Gabel, BDSG, § 4b recital 28.

Importance of a DPO

However, the DPO may help businesses to comply with data protection provisions and will provide orientation to employees on how to handle personal data. *Please read FAQ 7 for further details about employee training.*

- □ Consider the need to appoint a DPO or designate a point of contact within your organization responsible for data protection issues.
- □ Remember that you are responsible for your data even if your CSP has its own DPO or point of contact for data protection issues.

FAQ 9 - Sub-contractors

Most cloud users want to know what should be taken into consideration regarding possible sub-contractors of the CSP.

Who is considered to be a sub-contractor?

In most cases, cloud users are not sure whether the cloud services are provided exclusively by the CSP with whom they have entered into the cloud service agreement, or whether any further sub-contractors are involved. Sub-contractors include any further persons or companies that are engaged in order to support the CSP to perform its contractual obligations. These obligations derive from the prime contract between the cloud user and the CSP.

Often, the agreed cloud services can only be provided with the involvement of sub-contractors. However, there are some CSPs who do provide their cloud services without any sub-processing.

- □ Ask your CSP if any sub-contractors are involved.

Liability issues in case of sub-contractors

If your CSP does not use sub-contracts, then this topic does not pose a concern for you

- □ Where the CSP uses sub-contractors, please check that the required contracts are in place.

Content of a data processing agreement with sub-contractors

Between the CSP and any possible sub-contractor located within the EEA/Switzerland, a written data processing agreement[57] should be in place with sub-contractors. According to section 11 (2) BDSG, this agreement should set out the details concerning the data processing. These details should include the specification of the collection, processing and use of the data, the technical and organizational measures and any sub-commission.

- □ Check that the contract with the sub-contractor guarantees the level of data security as described in the main contract between you and the CSP and includes all relevant issues as described in section 11 BDSG.

[57]https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Auftragsdatenverarbeitung/Inhalt/Mustervereinbarung_zur_Auftragsdatenverarbeitung_nach____11_BDSG/Mustervereinbarung_zur_Auftragsdatenverarbeitung_nach____11_BDSG.php, as consulted 22.09.2016.

Data processing agreement with non-EEA/Switzerland sub-contractors

Moreover, where sub-contractors are located outside the EEA/Switzerland and a data transfer takes place, an appropriate data transfer contract regulating international issues should be signed. Based on the European Directive 95/46/EC58 and the General Data Protection Regulation (GDPR)[59], data processors located within the EEA/Switzerland are not permitted to transfer personal data to a country outside of the EEA/Switzerland unless the recipient is able to guarantee the same level of data protection. Currently, a data transfer data outside of the EEA/Switzerland is accepted if:

- the transfer is based on an adequacy decision from the EU Commission, e.g. EU-U.S. Privacy Shield[60], other countries with approved adequate data protection level[61], or
- there are appropriate safeguards regarding the transfer in place, e.g. Standard Contractual Clauses (SCC) or Binding Corporate Rules (BCR)[62].

– □ In case the data is processed outside of the EEA/Switzerland, it is suggested to implement Standard Contractual Clauses[63] to make sure that the same level of data protection is guaranteed by your service provider and its sub-contractors.

If Standard Contractual Clauses are in place between the cloud user and the CSP, all sub-contractors are obliged to act as directed by the cloud user in the main contract with the CSP, according to Clause 11 (Sub-processing) of the SCC[64]. In this case, the data should be processed as originally agreed with the cloud user and this obligation will be transferred to any further sub-processors[65].

– □ Moreover, check whether the technical and organizational measures are correctly implemented, documented and updated by the sub-contractors. Certifications could be used. *Please read FAQ 1 for further details about on-site audits.*

[58] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[59] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en, as consulted 22.09.2016.
[60] https://www.privacyshield.gov/US-Businesses, as consulted 22.09.2016.
[61] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, as consulted 22.09.2016.
[62] http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm, as consulted 22.09.2016.
[63] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 14.
[64] Commission Decision C(2010)593, Controllers to Processors transfers, (repealing Decision 2002/16/EC); http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, as consulted 22.09.2016.
[65] Arbeitskreise Technik und Medien, Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises; "Orientierungshilfe – Cloud Computing", p. 14.

Bibliography

Arbeitsgruppe „Rechtsrahmen des Cloud Computing“	Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing	10/2012
Arbeitskreise Technik und Medien, der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises	Orientierungshilfe – Cloud Computing	10/2014
Article 29 Working Party WP 196	Opinion 05/2012 on Cloud Computing	adopted on 01.07.2012
Bundesdatenschutzgesetz	(Federal Law Gazette I p. 66), as most recently amended through article 1 of the Act of 25.02.2015 (Federal Law Gazette I p. 162).	in the version promulgated on 14.01.2003
Datenschutz und Datensicherheit	Die Kontrollpflicht nach § 11 Abs. 2 Satz 4 BDSG im Zeitalter des Cloud Computing	04/2013
Fraunhofer Institute for Secure Information Technology	SIT Technical Reports on the Security of Cloud Storage Services	03/2012
German Federal Office for Information Security	Cloud Computing Compliance Controls Catalogue (C5) – Criteria to assess the information security of cloud services	02/2016
German Federal Office for Information Security	M 2.167 Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten	state 2016
German Federal Office for Information Security	M 2.433 Überblick über Methoden zur Löschung und Vernichtung von Daten	state 2011
German Federal Office for Information Security	Cloud: Risiken und Sicherheitstipps	state 2012
German Federal Office for Information Security	Eckpunktpapier – Sicherheitsempfehlungen für Cloud Computing Anbieter	02/2012
http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm	Binding Corporate Rules	as consulted 22.09.2016

http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm	Standard Contractual Clauses	as consulted 22.09.2016
http://eur-lex.europa.eu/legal-cotent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en	European Regulation 2016/679	as consulted 22.09.2016
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML	European Directive 95/46/EC	as consulted 22.09.2016
http://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/Was_ist_Datenschutz/Artikel/Datengeheimnis.html		as consulted 21.09.2016
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/CloudZertifizierung/CloudZertifizierung_node.html	Cloud Zertifizierungen	as consulted 22.09.2016
https://www.cogress.gov/107/plaws/publ56/PLAW-107publ56.pdf	USA Patriot Act	as consulted 22.09.2016
https://www.cogress.gov/114/plaws/publ23/PLAW-114publ23.pdf	USA Freedom Act	as consulted 22.09.2016
https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Auftragsdatenverarbeitung/Inhalt/Mustervereinbarung_zur_Auftragsdatenverarbeitung_nach____11_BDSG/Mustervereinbarung_zur_Auftragsdatenverarbeitung_nach____11_BDSG.php	Mustervereinbarung zur Auftragsdatenverarbeitung nach § 11 BDSG	as consulted 22.09.2016
https://www.privacyshield.gov/US-Businesses	Privacy Shield Framework	as consulted 22.09.2016
Teager/Gabel	BDSG	07/2013

Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Str. 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com