EuroCloud Deutschland_eco e.V.

Guidelines Cloud Computing German Law, Data Protection & Compliance

1. Imprint

EuroCloud Deutschland_eco e. V.
Lichtstrasse 43h
50825 Cologne
Germany

Tel.: +49(0)221 / 70 00 48 – 0
Fax: +49(0)221 / 70 00 48 – 111
E-Mail: info@eurocloud.de
Web: www.eurocloud.de

Register of Associations:
Cologne District Court – VR 16215
Seat of the Association: Cologne

Content

2. Foreword

Dear Readers,

Innovation is the engine of an economy, and positioning for innovation is what fuels economic success. Cloud computing is clearly a major trend and major evolutionary development of the Internet that customers and suppliers alike stand to benefit greatly from in the future. Cloud computing signifies a dawn of a new age for the Internet, opening doors to an entirely new world for how IT is utilised.
When new innovative solutions are brought to market, particularly those that distort and revolutionise an entire industry landscape, uncertainty often ensues. This uncertainty lies with new providers of course, but particularly with those that purchase and use new services that emerge from a new environment. Services that emerge from the cloud are no different and face the same uncertainties.

Cloud computing is an especially attractive option for midsized companies, often lacking the resources to individually test external providers, as it allows them to remain competitive and expand in areas, where previously they were unable. However, these companies still often do not have the sufficient resources or expertise to personally examine the potential legal implications for the use of cloud services and how their relationships with external providers in this area should operate. The question is, how should cloud computing contracts with appropriate legal, data protection, provider, terms, be designed?

Initially, if appropriate, cloud services shall become offered and utilised transnationally. However, the often widely discussed and undying issue of security of the Internet, is an equally concerning issue within the cloud. Uncertainty over security problems in the cloud are arguably even more pertinent than the legacy concerns for the Internet as a whole, owing to the cloud's infancy. Technological requirements for a secure service delivery are therefore absolutely essential. However, the providers partially prevailing in Europe, do not always have clear, or basic, framework conditions. A thorough audit is required for a national and European legal framework for a global service delivery from the cloud.

With the launch of the EuroCloud Deutschland_eco e. V. in February 2010, a Legal Expert Group was set up to prepare for the sometimes complex legal issues surrounding cloud computing. The aim was to provide users and providers of cloud services guidance in the areas law, data protection and compliance, and provide support. The results are evident in this guide, “Cloud Computing: Law, Data Protection & Compliance”.

The technical expertise that this guide is based on, is also part of the neutral, independent certification “EuroCloud Star Audit Software as a Service”, which EuroCloud Deutschland_eco e. V. began offering to the market at the start of 2011.

We would like to thank the legal experts for the content and the eco - Association of the German Internet Industry team for helping co-ordinate the production of the guide.

Bernd Becker
Chairman, EuroCloud Deutschland_eco e.V.
Vice President EuroCloud Europe

3. Introduction

The association EuroCloud Deutschland_eco e. V. was founded in 2009 as a national organisation of the European EuroCloud network. With its connection to the eco Internet Association which has been in existence since 1995, an ideal partnership for the support of cloud computing issues was achieved. Cloud computing is a global issue and holds an important status in the planning of future IT strategies.

Security and compliance are the two most important issues that stand out from the many that exist. With the initiative "SaaS Quality Seal" and by working out the fundamentals of the legal background, EuroCloud has started important projects to improve the general framework for a successful implementation of cloud services in different areas (software, platform and infrastructure).

This guide is a basis for the correct classification of the legal requirements and focuses on the area of Software as a Service as a "public cloud service". This has resulted in the emergence of special requirements pertaining to data protection, which schould always apply to all SaaS applications.

The overview of topics is derived from the test criteria used by the EuroCloud SaaS Quality Seal which is a thorough test of "Software as a Service" products, in terms of service, data security, data protection, contract terms, and interoperability.

4. Legal Requirements

A main concern under "Law and Compliance" in cloud computing is data protection. The guideline looks at issues particular to data protection that arise from contractual agreements between user and provider.

The data protection guidelines become relevant when personal data such as customer data or employee data are affected. What needs to be considered is the fact that "personal data" is defined very broadly in the German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG). All data that relates to an identified individual, or to an individual that can be identified by providers, users, or third parties, is defined by the data protection authorities as "personal data." In practice there will only be a small number of applications that do not at least partly process personal data.

Contracutal issues (governed by civil law) pertaining to SaaS services, including for instance service levels, liability limitations and termination provisions are not part of the following elaborations.

The following are guidelines on implementing data protection requirements (section 11 of the Federal Data Protection Act) in contracts between providers of SaaS / cloud computing and their customers. These guidelines relate mainly to specific data protection issues around cloud computing, offering different approaches to cloud spacific compliance for the processing of personal data.

To begin with, the following must be considered:

- The customer remains responsible for the legality of the processing of data within the framework of using the cloud computing services, according to section 11 of the Federal Data Protection Act. The customer may only use the service to process personal data to the extent he was allowed to process such personal data before using such a service.

» In cloud computing, the user, therefore the customer, is responsible for the lawful processing of data (section 11 of the Federal Data Protection Act)

- Signing an agreement pertaining to data processing as a basis for data protection is also necessary when the cloud computing application is only being tested. In order to avoid the cost and effort of such an agreement, there is the option of performing tests without using real data.

» Even when a cloud computing application is only tested, a contract must be entered into with the provider when real data is processed.

› German data protection authorities see cloud computing and SaaS solutions with a critical eye and foresee some problems, especially in the areas of control and instructions by the customer, technical measures, data processing locations, using subcontractors and using data centers outside of the European Economic Area. However, even German data protection authorities do not completely reject cloud computing and SaaS. The guideline provides practical solutions that are currently considered for data protection specific problems and are seen by the authors of the guideline as appropriate.

5. Main Issues Pertaining to the Cloud Provider Selection

» The customer is required by law to carefully select the provider.

» After the contract is concluded, the customer must regularly check if the provider is complying with the necessary technical and administrative measures.

The customer must carefully select the provider and must be satisfied before the data processing begins (and regularly thereafter) that the provider takes and respects appropriate technical and organisational measures.

In practice, that means that the user must have a look at the provider before an agreement is signed and ascertain that the provider is the appropriate one in order to fulfil its legal obligation to carefully select the provider. This process can be easier if the provider fulfils the standards of a quality seal or has an outstanding reputation.

6. Main Parts to a Contract Regarding Data Protection

6.1 Form

» The contract must be in writing, concluding a contract online with qualified electronic signatures is possible.

A valid contract requires the written form. In practice, this means that the contract is signed by hand by both customer and provider, or qualified electronic signatures are used.

A possible option for concluding an online contract if the strict requirements of a qualified electronic signature are not fulfilled: Upon request, the customer receives, without undue delay, a written contract signed by a person authorised by the provider, which is identical to the online contract. It may be clarified that rights and obligations (for example payment of fees) arising from the contract remain valid even without a written contract.

6.2 Subject Matter of the Contract

The type of service must be roughly described. As far as the handling of personal data is concerned, detailed descriptions are needed (for example hosting, operation, maintenance and

enabling online access to a certain application, data migration). With regard to parameterisation and customising, it needs to be distinguished whether this is taking place before or after the personal data is entered.

When drafting the agreement in practice, the legal obligation to establish what data will be processed (section 11, paragraph 2, page 2, number 1 of the Federal Data Protection Act) is fulfilled together with the obligation to stipulate the extent, the type, and the purpose of the intended collection, processing, or use of data, the type of data and the affected persons (section 11, paragraph 2, page 2, number 1 of the Federal Data Protection Act).

» *If personal data is affected, the type of service must be described: hosting, operation, migration of data?*

» *Customising: Does this take place before or after the transfer of personal data?*

As long as the functional description, or the provider's general data protection information, shows which data, and how this data, is collected, processed and used within the framework of the particular application, a reference may be made to these documents. An individual description of the services with regards to how the personal data is handled would be preferable however with cloud offers this is often not particulary pragmatic.
A mere reference to the existing (and possibly customer tested) application, or to online user manuals, however, is insufficient as this can be unilaterally changed by the provider. This may be assessed differently if the particular version is explicitly noted and documented.

» *Is personal data processed? If yes, how?*

The following aspects should be examined closely:

- Clarifying if, and possibly how, "special types of personal data", according to section 3 paragraph 9 of the Federal Data Protection Act, are collected and/or used. Special types of personal data are classified as information on race and ethnic background, political opinion, religion and philosophical convictions, union activity, health or sexual life. When such data is processed advice should be sought on a case by case basis.
- Description of third parties, which can have access to data (through interfaces, as maintenance companies, subcontractors etc.).
- Clarifiying that data can be deleted at any time at the request of the user and how this takes place.

» *What third parties have access to it?*

» *Note, that data can be used at any time on request of the client.*

6.3 International Data Processing (Including Using Foreign Resources and Subcontractors)

The Federal Data Protection Act privileges commissioned data processing by inputting the data processing of the contractor to the client and waiving the requirement of a permissive rule for transferring data to the contractor. This beneficial exemption

» *Customer data can only be readily processed by contractors (company accepting the order) located in the EU or the EEA.*

however, only applies if the service provider is based in the EU or in the EEA (section 3, paragraph 8, and page 3 of the Federal Data Protection Act). For commissioned data processing by service providers in such third countries – i.e. outside the EU or the EEA – or an actual processing of personal data in such a third country, additional requirements have to be met before a transfer of data to such a third country can take place:

The obvious option is to use the standard contract issued by the European Union, the so called standard contract clauses for data processing. Even though this contract does not have the same effect as a commissioned processing of data, as defined in the Federal Data Protection Act, it triggers the application of the same requirements for data transfers to third country recipients as it does for data transfers within the EU or the EEA.

However, German data protection authorities are demanding an addendum to this standard contract to include the contractual stipulations as required by section 11, paragraph 2 of the Federal Data Protection Act. This proves problematic as changes to the EU standard contract would lead to a loss of the effect described above (according to which international transfers are subject to the same requirements as transfers within the EU or the EEA). The implementation of these additional German requirements must therefore take place in a way that merely adds them to the (unchanged) EU Standard Clauses without limiting, directly or indirectly, the provisions of the standard contract. This way all the requirements would be fulfilled.

6.4 Liability

» *The responsibilities pertaining to data protection must be clearly defined in the contract.*

In the interest of the provider, the fundamental data protection responsabilities (the service provider is only the contractor, whereas the user is the customer and has the main responsibility, i.e. as if the customer would process the data by itself) are clarified in the contract and the user comits to only use the applications in a way that is compliant with data protection laws.

In the interest of the user, the contract should clarify that the user alone is in charge of outside communication – even in cases of data protection security breaches – and the provider, however, must immediately inform the user in detail about any data protection and/or security breaches.

The provider should encourage the user to clearly communicate to any affected external parties that the user is exclusively liable for claims raised by the affected individuals, especially if they request

information, correction or deletion of their data.

According to section 3, page 2 of the Federal Data Protection Act, the provider shall inform the user immediately if the provider considers a customer instruction as incompliant with data protection regulations. This provision will not play a very important part in the practice of cloud applications. The provider supplies the user with a standard application that rarely involves special instructions for the user from the provider in regard to handling personal data. However, it makes sense to clarify in the contract that the provider, in this case, will indicate that such a violation is taking place, however, that the provider will not carry out legal examinations and, in doubt, will still have to carry out the user's instruction. Visibly illegal instructions must in no case be carried out by the provider.

6.5 The User's Rights to Control

The provider must grant the user control rights. That means that the user must have the right to control via the provider – even on location – how the data processing is handled and what protection measures are taken, or have such controls performed by a third party. This applies to all locations where data is processed. In particular, if there are several, and distant, locations, an audit performed by a third party, such as within the framework of a certified, possibly standardised audit, would be an option. However, the data protection authorities (at least currently) are demanding that the user at least has the right to carry out individual audits. This should be regulated in the contract accordingly.

» The customer must reserve the right to perform checks on the contractor.

Above and beyond this control right, the user should also demand that the provider shall supply the data necessary for an audit and otherwise contribute appropriately to the auditing process. As a rule, the audits could be limited to business hours and a prior appointment. Typically, an appropriate audit can only actually be carried out under these conditions.

Moreover, if relevant, audits carried out by supervisory authorities should be contractually regulated as well.

Since this is a legal obligation to design commissioned data processing contracts, it does not make sense for the provider to reject such requirements. The provider should rather offer users appropriate standard procedures. However, the law does not stipulate that the support offered by the provider must be offered at no cost. So for a fair balance of interests, it may make sense to

regulate that the user carries the cost for an effort that goes above and beyond a certain level.

6.6 Technical Organisational Measures

» *Technical/administrative measures pertaining to the protection of personal data must be contractually and clearly defined.*

A legal requirement pertaining to the content of the contract for commissioned data processing is the stipulation of technical organisational measures to protect the processed personal data. The attachment to section 9 of the Federal Data Protection Act lays out which aspects must be regulated.

That means, a specific security concept meeting the actual requirements of the situation must be laid out in a contract that describes the provider's obligations. Abstract or general descriptions are insufficient; they must be specific to an extent that it is made clear which measures are being taken. These measures have to secure an appropriate level of protection, it being understood that for the evaluation of the adequacy of such protection measures, the actual processed personal data needs to be taken into account.

In practice the provider can create a security concept for its service that is then audited by the user and thereafter reflected by an appropriate contractual requirement. However, it is obvious that with standard SaaS or cloud offers an audit carried out by the user cannot result in specific user requests to be honored by the provider. The user is obligated to check if the security concept fulfils the data protection requirements and is in line with the sensitivity of the data before data is transferred to the provider.

The security concept has to be continually updated to match the technical development in order to maintain the level of protection.

Both user and provider are legally obligated to respectfully maintain this level of protection.

The user must verify before the data processing has started, that the provider has taken adequate technical-organisational measures in compliance with the Federal Data Protection Act. In the interest of both parties this can take place after the conclusion of the contract, i.e. the final selection, as long as the audit takes place before the beginning of the actual data processing. In practice this means that the necessary measures must have been obviously clarified at the conclusion of the contract.

It is not mandatory to verify compliance with these requirements at the location of the provider. This can also be achieved if the provider produces respective certificates, audit results or provider statements. The higher the need for data security from the point of view of the affected individuals (to whom the data relates to), the more thorough the verification of compliance should be.

After the initial verification this process has to be repeated regularly. This should be clarified in the contract. A specific time schedule is not set forth in the law. The appropriate schedule for verifications of the technical and organisational safety measures is therefore to be determined according to the sensitivity of the data (from the point of view of the affected individuals). In any case, a verification must take place when there are doubts that the protection measures are not being fulfilled by the service provider.

Moreover, legally, it is crucial that the verification process is well documented. The result of the respective verification has to be documented by the user. What must be documented is that the verification took place and the result.

The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) has published a draft "BSI – Minimum Requirements for Cloud Computing[1]", last updated 09.27.2010. The final version will be a recommendation. However, please note that this recommendation is not binding like a law. However, it will have an indirect legal relevance as a minimum standard for the understanding of open terms used in section 9 of the Federal Data Protection Act. The developments must therefore be followed closely.

6.7 Involving Subcontractors and Their Control

The Federal Data Protection Act requires the contract for commissioned data processing to deal with "the optional right to retain subcontractors." A subcontractor would be an entity retained by the provider that cannot be excluded from accessing the data processed for the user. A transfer of data directly to the subcontractor is not necessary. Access by way of remote data entry or remote data maintenance is sufficient. Moreover, it does not matter if the subcontractor is supposed to process the data, but rather if the subcontractor can actually access the data.

1 See "10.2 Cloud Computing und Compliance", page 30

» *The possible hiring of subcontractors must be contractually defined.*

The law requires only contractual rules on whether or not the provider may retain subcontractors. However, such a simple provision is not in line with the user's data protection requirements and it is also not understood in such narrow terms by the data protection authorities.

In practice, to satisfy both the provider's and the user's needs, it may be feasible to distinguish between categories of subcontractors. Therefore, certain categories would require prior approval, whilst in other categories, the involvement of subcontractors can take place without special approval as long as certain defined requirements are fulfilled. Regardless, the customer must be informed about the subcontractor and the subcontractor's activity.

The obligation to inform can be simplified if the provider maintains an access-protected list of subcontractors online, which the user can view and the customer can be notified of changes to the list by email. The list contains the name and address of the subcontractor and a short description of the services delivered by that subcontractor. The customer can request that the provider disclose the terms of the contract with the subcontractor that relate to data protection.

Retaining subcontractors is only admissible if the subcontractor warrants the same level of data protection that is agreed upon in the contract between the user and provider. As a result, the contracts between providers and subcontractors have to ensure the same level of protection as the contract between providers and customers, especially with respect to technical and organisational security measures. The provider should ensure this in its own interest in order not to "fall" into the gap between strict commitments given to the user and less strict obligations of its subcontractor.

When retaining subcontractors, the user should be aware that it remains liable for the services provided by a subcontractor in the same way as it does for its own performance.

The provider has to contractually ensure that it has the same control rights in relation to the subcontractor as those contractually afforded to the user.

6.8 Term and Returning Data

The term of the contract must also be specified. In this respect, no cloud specific issues arise. There is no need for a fixed term. The contracts can run indefinitely with the option to give notice of termination.

If the provider gives the customer data migration support, the period of migration also belongs to the term of the commissioned data processing relationship.

The contract must also provide rules with respect to the "returning" of personal data upon contract termination in relation to section 11, paragraph 2, page 2, number 10 of the Federal Data Protection Act.

The two basic scenarios are the transfer of data back to the user (and subsequent deletion from the provider's systems) or the mere deletion of data by the provider. The contract has to provide for an exit scenario without additional charges. Even after termination of the contract for the commissioned data processing, the contract should ensure that the data is handled in a way compliant with data protection requirements until the provider has actually deleted all personal data.

Already, when concluding the contract, the user should define its requirements for the return of data so as to enable the switch to another service provider or reintegration, e.g. requirements for a means of transmission (for example per sftp) and data form, or if explanations pertaining to the data structure will be necessary.

Besides this issue – which is also cost sensitive – the provider needs to define the point in time at which it will be able to delete the data if the user ceases to pay or becomes insolvent.

» *The contract must define the term and must define how data is returned.*

7. Product and Industry Specific Particularities

Special requirements may arise in certain cases e.g. for customers:

- from the financial services industry (section 25a of the German Banking Act, principles of computer based bookkeeping -GoBS -, section 20 of the Payment Services Supervision Act –ZAG-),
- from the telecommunications sector (Telecommunications Act – TKG-)
- who maintain official and professional confidences (section 203 German Penal Code: physicians, attorneys, life, health or casualty insurers),
- who process tax related data (sections 146, 147 of the German Tax Code – AO-, the principles of data access and verifiability of digital documents –GDPdU-, section 41 of the German Income Tax Act –EstG-).

7.1 Financial Services

The issues particular to the financial sector are briefly touched upon here but cannot be reviewed in a comprehensive manner: Section 25a, subsection 1 of the German Banking Act includes general business management obligations for credit institutions. Section 25a, subsection 2 of the German Banking Act defines these obligations in more detail in cases when activities and processes essential to the carrying out of banking business, financial services or other institution services are outsourced to another company.

For financial institutions in the sectors of securities, funds, and insurances, similar regulations apply as regulated in section 33 of the German Securities Trading Act –WpHG-, section 16 of the German Investment Act –InvG-, and section 64a of the Insurance Regulatory Act – VAG-.

Therefore, each individual case must be scrutinised to see if the cloud transferred tasks and processes are “essential” according to section 25a, subsection 2 of the German Banking Act and to see if they fall under the concept of “outsourcing.” If that is the case, also pursuant to section 25a, subsection 2 of the German Banking Act, appropriate data protection measures must be taken as well as excessive additional risks avoided (for example carefully selecting the cloud provider, monitoring the service, determining methods for the evaluation of the service as well as emergency planning.)

7.2 Telecommunications Act

From the perspective of the data protection authority, the cloud service option has other limitations in the telecommunications sector. Sections 95 ff of the Telecommunications Act is based on the principle that a transfer of personal data, user data and traffic data is only admissible with the consent of the person concerned. Consent from the person concerned is out of the question. There is the alternative of the concept of "processing personal data on behalf of others" (section 11 of the German Data Protection Act –BDSG). This, however, is limited to the EU and EEA countries according to section 3, subsection 3 of the German Data Protection Act. Stepping over these limits is problematic in terms of cloud services. Moreover, the argument could be made that section 92 of the Telecommunications Act draws a further line by limiting the scope of data processed on behalf of others pursuant to section 11 of the German Data Protection Act to rendering telecommunications services, generating and mailing invoices as well as combating fraud. In legal terms it is argued whether section 92 of the Telecommunications Act actually contains such a delimitation as it is only supposed to clarify the areas of application of section 11 of the German Data Protection Act.

7.3 Accounting Obligation

When tax related data is used by cloud providers, sections 146 ff of the German Tax Code must be considered. Section 146 of the German Tax Code says that tax related "books and notations" must always be maintained and kept in the original inside the country. The relocation to a foreign cloud has previously only been possible as an exception on the basis of "approved facilitation" pursuant to section 148 of the German Tax Code or by virtue of tolerance shown by pragmatic fiscal authorities.

In the past, however, both scenarios have been handled by the local fiscal authorities in very different ways. That changed on 01.01.2009. According to subsection 2a added to section 146 of the German Tax Code on 01.01.2009, the relevant fiscal authority, upon request, can approve electronic bookkeeping to be done in an EU member state or in an EEA member state by way of an administrative assistance agreement if the foreign fiscal authority has given its consent and if the German fiscal authority is granted access pursuant to section 147, subsection 6 of the German Tax Code. However, what remains to be seen is if the new regulation has improved the situation. On one hand, as expected, the first mentioned prerequisite created problems in practice. On the other hand, the regulation represents a solution for cloud services only for clouds inside the EU/EEA.

In view of the explicit regulation in section 146, subsection 2a of the German Tax Code, the question arises whether the solutions previously used in practice ("facilitation" according to section 148 of the German Tax Code, "tolerance" –see above-) will remain an option, or if the fiscal authorities will see section 146, subsection 2a of the German Tax Code as a final special provision and if that will hinder global clouds.

At any rate, the obligation to show and keep detailed operation documentation available at all times pursuant to section 147 of the German Tax Code remains.

The problem arising in this context is the actual availability of data. Regulations for audits should therefore be agreed upon with the cloud provider.

7.4 Legal Obligation to Keep Records Under Commercial Law

According to the Code of Commercial Law (HGB) every business must keep records of transactions for a period of ten years pursuant to section 238, subsection 1 of the Code of Commercial Law. This is also possible in an electronic format on data storage devices and in clouds pursuant to section 257, subsection 3, of the Code of Commercial Law (HGB). Under commercial law there is no obligation to keep records inside the country. According to section 257, subsection 3, number 2 of the Code of Commercial law, however, the electronic records must be made available for reading within a reasonable time period.

7.5 Persons Subject to Official and Professional Confidences

In sectors with special obligations of secrecy pursuant to section 203 of the German Penal Code (for example in the sector of legal counsel, in the health sector, health, casualty and life insurance) the admissibility (and therefore culpability) of outsourcing to third parties, for example cloud providers, is controversial. The central starting point for admissibility is the interpretation of the "assistant" concept in section 203, subsection 3, page 2 of the German Penal Code since a transfer without the consent of the data subjects is (only) admissible to "assistants."

According to the traditional interpretation such assistants are not people who are self employed. Therefore, cloud computing in the sense of section 203 of the German Penal Code could hardly be possible. It would be more appropriate not to define an assistant by the self employed characteristic but rather to establish if the person/entity holding the primary obligation of secrecy maintains control over the provided data. The criteria of section 11 of the Data Protection Act could be evaluated for this purpose. That integrates the third party into the scope of "informational self-determination" and can be viewed as someone who is part of the "circle of people privy to information." Prohibiting such an outsourcing is therefore not advisable when the strict criteria of section 11 of the Data Protection Act are respected before the protection of section 203 of the German Penal Code. However, it is not yet clear if the admissibility is legally binding.

8. Checklist Law & Compliance

Following the EuroCloud SaaS Quality Seal, the most important questions pertaining to the contract format are listed. Providers reviewed, according to these guidelines, fulfil the basic requirements necessary to offer cloud services in conformity with the law.

Currently there are already a variety of professional and secure solutions. The quality seal will offer providers the important help necessary to win the trust of users with fair terms.
There must be a clear disassociation from providers who take the bare minimum route as the user can only find out about the real deficits with great effort and, in the worst case scenario, only after things have escalated.

The following categories are targeted by the quality seal:

- Provider Profile
- Contract and Compliance
- Security
- Infrastructure Operations
- Operations
- Application
- Implementation

A provider can achieve quality levels from one to five stars via a points system and minimum criteria.

As opposed to other initiatives, whereby only parts of the whole picture are taken into considerations or the information provided is not cross checked and is seen as voluntary, the SaaS Quality Seal is granted only after the provided information has been validated and the validation repeated at agreed upon time intervals in order to have concrete proof of the validity of the information. Moreover, the providers make a commitment to immediately report significant changes to the framework conditions (for example place of service rendered, changes to subcontractor agreements) as well as critical incidents.

The SaaS Quality Seal will be officially awarded starting at the beginning of 2011 and a number of providers are currently preparing for the certification.

8.1 Conclusion of the Contract and Contract Format

- How is the contract concluded?
  - Online
  - In written form
- Can the customer insist on a written contract?

8.2 Effect for Subcontractor

- Did the provider commit the subcontractor to the same obligations that the provider has to the user?

8.3 Billing

- Is the use of services billed at a flat rate time-dependent?
- Is the use of services billed on consumption calculated?
  - Are there quantity discounts/different prices depending on the amount of used services?
  - Can the provider change their prices in cases when the usage volume changes significantly?
  - Is there a best price option?
- Is an optional flat rate or per user flat rate offered?
- Are there special services billed separately?
- If yes, which

8.4 Performance Disruptions

- Provider or Subcontractor Performance Disruptions
  - Are damages regulated in case of performance disruptions?
- Disagreements Over Performance / Payment Default
  - Is a right to user data retention or performance refusal contractually excluded?
  - In case of disagreements over performance or payment default, is it excluded that the provider delete the data without the user's permission?

8.5 Contract Termination

- Which periods of notice are defined for the provider and the user?
- Is there a non-exhaustive list of possible termination reasons?

- Is termination for an important reason possible?
  - If yes, for who?
    - User
    - Provider
    - Why?

- Subcontractors contractually regulated?

- Does the user have a special termination right if the provider switches important subcontractors?

- Are there rules pertaining to the participation of the user in the process of data provision after the termination of the contract?

8.6 Provider Insolvency

- Are there rules in place to protect the user data and the availability of the application in case of provider insolvency?
  - Source Code Deposit?
  - Is the software bound to a certain platform?
  - Does the user have a right to demand the last data backup and documentation?

8.7 Compliance

- GDPdU[2] (Principles of Data Access and Verifiability of Digital Records) Relevance
  - Are applications operated as SaaS bound to GDPdU (Principles of data access and verifiability of digital records)?
    a) Does the application include the processing of electronic billing?
    b) Within the scope of the application, is there data that is processed that flows directly into the accounting of the provider?

- GDPdU (Principles of Data Access and Verifiability of Digital Records) Ability
  - If applications are operated as SaaS bound to GDPdU: are the user's obligations towards the tax authority supported by the provider?
    - If a): Are the guidelines regarding the signature validation and billing storage transcribed in the original and in the in-house format?
    - If b): does the application offer the option of data access in all three prescribed types of access (Z1, Z2, Z3)?

2 Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

- If b): does the role concept of the application offer an auditor role who has been assigned the read access of the outside auditor?
- If b): is the tax relevant data identified within the application?
- For a) or b) Does the provider deliver adequate procedure documentation?
- For a) or b) AND when an archiving system is used for aged data: Does the archiving system have the same access and processing options as the productive system?

- Data Protection Relevance
  - Is personal data in the sense of the Federal Data Protection Act processed within the application?

  ONLY IF YES, please answer the following questions.

  Please note that the term "personal data" as worded in the Federal Data Protection Act is very broad. All data that is related to a person (identifying data) or data that can be used by the user, provider or a third party to identify a person is data defined by the point of view of the data protection authority as "personal data". In practice, there are only very few IT and cloud applications processing data that is, at least partially personally identifying.

- Data Protection Organisation
  - Does the provider have a data protection officer who is available to the user as a contact person regarding all data protection issues pertaining to the provider and his subcontractors?
  - Are the employees of the provider obligated to maintain data confidentiality according to section 5 of the Federal Data Protection Act?
  - Has it been settled who will be the contact person for the user's customers pertaining to data protection?
    - Are rules defined as far as the correction, deletion and blocking of data where the request of an affected party is concerned?
  - Provider and Subcontractor Selection
    - Does the provider offer sufficient information about his companies and subcontractors in order to enable the user to make an informed provider selection according to section 11, page 1 of the Federal Data Protection Act?
    - Are the names of the subcontractors disclosed?

- Level of Data Protection
  - If relevant, is there an adequate level of data protection outside the EU pertaining to participating subcontractors, for example through an EU standard contract or safe harbor regulation?
  - Does the option exist to limit the locations of data storage to Germany or the EU, and if so, is it dictated by legal or authority requirements?

- Commissioning and Right to Give Instructions
  - Are the responsibilities between provider (fundamental data protection responsibility) and user (implementation of instructions, technical protection measures) clearly defined?
  - Is the scope of the data processing order sufficiently and clearly specified? In particular:
    - Is the service described in broad terms? Does the description document the scope, time and purpose of the intended collection, processing or usage of data, the type of data and the circle of affected parties?
    - Is the duration of processing and the deletion of data exactly defined?
    - Is a provider scope in decision making pertaining to data processing excluded?
    - Is it documented if, when and how "special types of data", with regards to section 3 of the Federal Data Protection Act, are collected, processed or used?
  - Is the user's right to give instructions clearly defined?

- Communication
  - Is a rule of communication established in case the user's instructions violate data protection from the point of view of the provider?
  - Is it defined what situations have to be reported to the provider e. g. personal data protection violations caused by the user or his employees or violations of the agreement?

- The Implementation of Technical and Organisational Data Protection Measures
  - Does a documentation concept exist to implement technical and organisational measures as required by the addendum of section 9 of the Federal Data Protection Act?
  - Does the user have to agree to this concept and possible changes to the concept?

- Options for the User to Exercise Control
  - Are there any rules pertaining to control rights of the user and to the respective tolerance and participation obligations of the provider, especially:
    - Have a user's control rights, and / or the control rights of a third party commissioned by the user, been expressly agreed upon at the location of the provider or one of his subcontractors?
    - Are there (cumulative or as an alternative to user controls) regular controls/audits and certifications in place that control and certify the provider's data protection obligations to the user?
    - Is there a regulation pertaining to the participation of the provider and the connected cost?

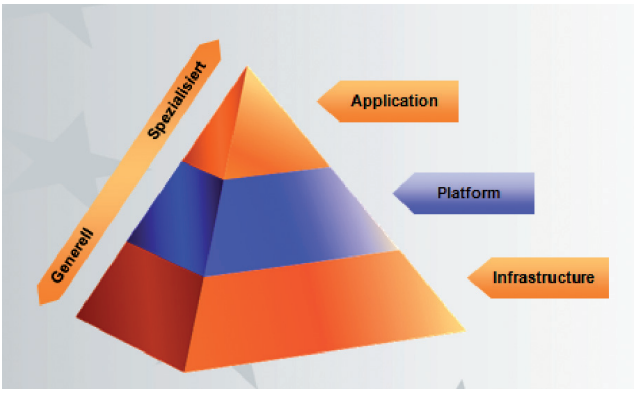
- Data Deletion at the End of the Contract
  - Are there rules in place pertaining to the deletion of data and the returning of data after the termination of the contract?
    - Is it warranted that the data is actually deleted when the user requests it?

9. Cloud Computing Glossary

Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Definition: NIST; National Institute of Standards and Technology, USA).

The different elements of cloud computing are often depicted with the help of the SPI model which illustrates the three service levels, infrastructure, platform and software:



The levels are built on each other however the lower levels can be used independently.

Public Cloud

IT-services are offered by the cloud provider and can be used by anyone over the Internet.

Private Cloud

IT-services are drawn from one's own computer center. All services and infrastructure are under the control of an institution. The cloud may be managed by a third party. The services are accessed either over the Internet or over a VPN (Virtual Private Network).

Hybrid Cloud

A mix between a public cloud and a private cloud.

Federated Cloud
Hybrid cloud with special security technology from trustworthy service providers in the area of identification and encryption.

Infrastructure as a Service
Providing computing and storage capacity as a service.

Platform as a Service
Providing middleware as a service

Software as a Service
Providing applications as a service.

X as a Service
Providing additional functions such as business operations, networks, communication and others as a service.

10. Sources

Legal Topics

- Weichert, Cloud Computing und Datenschutz, DuD 2010, 679, 679
- Niemann/Paul, "Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud-Computing", K&R 2009, 444
- Niemann/Hennrich, "Kontrollen in den Wolken? Auftragsdatenverarbeitung in Zeiten des Cloud Computings", CR 2010, 686
- Niemann, "Cloud Computing & Recht", Deutscher Anwaltsspiegel, Ausgabe 08/2010, 14
- Bierekoven, ITRB 2010, 42
- Pohle/Ammann, CR 2009, 273
- Bergmann/Möhrle/Herb, Datenschutzrecht, 40. Ergänzungslieferung – November 2009, § 11 BDSG, Rn. 15a

Cloud Computing und Compliance

- ENISA Cloud Computing Risk Assessment: **http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment**
- BSI – Eckpunktepapier Cloud Computing: **https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Cloud_Computing_28092010.html**

Order Data Processing

- It is advised to have a special privacy policy to accompany the contractual arrangements. A similar template is available from the company for Gesellschaft für Datensicherheit und Datenschutz e. V. (Data Security and Privacy e. V.): **https://www.gdd.de/nachrichten/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg**

11. Legal Notice

1. General

The information provided in this guideline is meant to illustrate the legal frame conditions for cloud computing, but it is not to be regarded as legal counsel and cannot replace legal counsel as such counsel requires knowledge of all particulars especially the particulars of each individual case.

2. Guideline Contents

The publisher/the authors assume no liability for the provided information to be complete, correct or up to date. This particularly applies to developments pertaining to jurisdiction or legislative changes. Liability claims against the publisher/authors pertaining to material or non-material damage arising from the use or disuse of the provided information or arising from the use of erroneous and incomplete information are excluded unless the publisher/ authors have verifiably acted deliberately and grossly negligent.

3. Notices and Links

For direct or indirect references to content derived from other sources such as links that are outside the area of responsibility of the publisher/the authors, liability would exist exclusively in the case that the publisher/the authors have knowledge of the contents and it is technically possible and reasonable to prevent the usage if the content is illegal. The publisher/the authors hereby declare that at the time of linking there were no visible illegal contents on the pages to be linked. The publisher/the authors have no influence over the current or future format, contents or copyrights of the linked pages. They expressly disassociate themselves from all contents on all linked pages that were changed after the links were added. The provider of the linked page alone is liable for illegal, erroneous or incomplete contents and especially for damage arising from the use or disuse of such information; the party merely referencing to a publication by adding a link is not liable.

4. Copyright

The copyrights of contents illustrated on this website such as texts, graphics or pictures are protected under the German copyright law. Any use prohibited under copyright laws requires the prior approval of the publisher. Third party segments are marked as such. This pertains particularly to copying, processing, reproducing contents in data bases or other electronic media. Unauthorised copying or disclosing individual parts of the guideline or the entire guideline is prohibited. The exception is the individual/private use; the private use does not include the right to circulate to third parties. The same applies to publications and other work.

12. Authors

Attorney Dr. Jens Eckhardt
JUCONOMY Lawyers,
Dusseldorf

Attorney Dr. Marc Hilber LL.M
Partner Oppenhoff & Partner,
Cologne

Rüdiger Giebichenstein
KPMG AG Accountancy Firm,
Cologne

Attorney Dr. Fabian Niemann
Partner Bird & Bird LLP,
Frankfurt

Attorney Dr. Thomas Helbing
Helbing Law Firm, Munich

Andreas Weiss
Director EuroCloud
Deutschland_eco e. V.

Notes

EuroCloud Deutschland_eco e.V.
Lichtstrasse 43h
50825 Cologne
Germany

Tel.: +49(0)221 / 70 00 48 – 0
Fax: +49(0)221 / 70 00 48 – 111
E-Mail: info@eurocloud.de
Web: www.eurocloud.de