Transcending the Cloud

A Legal Guide to the Risks and Rewards of Cloud Computing

Cloud Computing – A German Perspective

ReedSmith

reedsmith.com

Cloud Computing – A German Perspective

Chapter Authors

Thomas Fischl, Counsel – tfischl@reedsmith.com

Katharina A. Weimer, Associate – kweimer@reedsmith.com

Introduction

Traditionally, companies have devoted significant percentages of their overall budget to managing, supporting and scaling their own IT systems and networks. A company's growth and the size of its IT infrastructure typically have had a direct correlation. Until recently, a company's IT infrastructure options were restricted to incrementally scaling up internal capacity or outsourcing to third parties, all or some portion of the IT infrastructure. While the build vs. buy paradigm offers a variety of benefits and challenges, the balance—indeed the benefits and challenges—are in a constant and dynamic state of review and re-evaluation. Especially in an economically challenging environment, companies eagerly search for new solutions to their IT sourcing challenges—solutions that offer reliability, scalability, security, and a difference in their capital and operating expense budgets.

Cloud computing has recently risen to the forefront as potentially one of the most dynamic and most flexible solutions, to solve these companies' IT infrastructure needs with an innovative, cost-effective model. Cloud computing is the term ascribed to the industry shift and transformation from companies either hosting and managing their own applications and data on local servers, or entering into hosting arrangements with third-party providers, to a grid computing model in which users access a shared computing environment typically being provided by large and well-entrenched technology companies.

As we explain below, cloud computing may not necessarily be the silver bullet for German companies or companies doing business in Germany, even if and when it may indeed be an attractive alternative and viable option.

Duties of the Customer

Companies that arrive at the decision to host all or some of their systems within a cloud computing environment will have responsibilities both before the transition and throughout, and these commitments are often paramount to the success of their experience. Principally, customers must identify the nature of the cloud services best suited for their needs (public vs. private cloud hosting), both current and future, and source them from a cloud computing provider that is best able to carry out those services. Great attention to detail is necessary, and the individual departments within a customer's organization must cooperate and communicate with each other to understand both the micro- and macro-issues, and also paint a complete picture of the levels and types of services, hosting and support that the business units require.

Moreover, as a company's needs become more narrowly tailored and specific to certain types of applications, levels of security, support, and the like, the company must either be prepared to negotiate them into the cloud computing agreement or assume them itself and explore means by which the company can work alongside whatever service and support is being offered by the cloud computing provider.

Another fundamental responsibility (and perhaps the foremost such duty) that each cloud computing customer must understand and embrace is the continuous supervision that is required to monitor a company's cloud service. Cloud computing will often afford a customer the ability to change its IT staffing needs, but not eliminate them altogether. Furthermore, depending on the industry and regulatory requirements under which a company may be subject, there may very well be a statutory obligation on the party of the customer to monitor its network, data and suite of technology that has been moved onto some provider's cloud. If the customer cannot adequately supervise the provider itself, it must delegate this obligation to a third party who can.

Lastly, while cloud providers are generally well equipped to provision cloud computing services, a customer must still be certain that it has the requisite bandwidth, capacity, know-how and personnel to host and operate whatever

systems, applications and services remain internally. Customers should also be prepared for change—in terms of protocol, process and security. That which existed previously might be very different from a cloud provider's requirements, and rather than run into a constant state of conflict with the provider, a customer may simply have to change the way it does business in some respects.

Key Concerns of Customers

Cloud computing raises many questions for all parties involved. Customers will generally concern themselves with the following topics:

Contractual Parties

A German customer is likely to prefer a single German provider with whom it enters into a cloud computing services agreement, as the legal implications on many levels will be less onerous and worrisome. A customer will also likely aim to have a single contractual partner that is able to provide a one-stop, turn-key service instead of having to source services from amongst various providers (German or otherwise). While sourcing from various providers might provide a more tailored cloud experience and service, the resources a customer would require to coordinate and monitor its different cloud providers will likely be burdensome and eliminate any cost saving realized through the cloud. Additionally, error-free service is difficult enough to achieve with one provider, but having to coordinate different systems, programs, interfaces, and even operational approaches amongst several providers would likely trigger a multitude of errors, the detection of which could be very challenging.

Support

Support is often neglected in contractual arrangements, but is vital in the daily use of the cloud, particularly at the outset. Customers should seek to have personal support available to them at least during regular business hours, via phone, email and the Internet, and especially in case of emergency. The transitions involved in integrating new IT services, from file transfers to implementation, security, and privacy audits to account creation, often require some level of hands-on support. A customer must ensure and feel comfortable that a provider has the resources to carry out these tasks, and systems and processes are firmly in place to avoid business interruptions.

Right to Use vs. Obligation to Use

The customer should ensure that it is able to use the cloud services at any time and for any amount of time, without the obligation to use and/or pay for them continuously.

Scaling of Services

Even prior to a the onset of contractual negotiations, customers and their service providers must communicate and have some understanding of their needs both in the present and future, and must ensure that a provider will be able to meet those needs if and when they arise. By not having this conversation as early in the process as possible, customers may find themselves having to either add other providers to their hosting stable or move their entire system elsewhere, thus entailing considerable effort. The parties should feel reasonably comfortable that a provider possesses the ability to expand the scope of its services when necessary in return for appropriate consideration. If the provider is unable to commit to offering extended services, the customer may wish to consider other providers.

Sub-Contractors

The cloud provider needs to ascertain whether it can provide all services within its own structure or whether it requires the support or facilities of sub-contractors for certain services. The customer, in turn, should determine for itself whether it is willing to accept a series of secondary service providers, all of whom answer to a single primary provider, or whether it should continue to look for one very large cloud computing provider that either, itself, has a large enough cloud, or one that has a global footprint.

Access to Own Data

The customer must have access to its data at all times, and it is crucial that the data be in a format that other applications can process. The agreement should also plan for the unlikely event of a termination, a provider's refusal to cooperate and/or its insolvency. In all of those potential scenarios, mechanisms should be put into place to ensure continuous availability and access of the customer's data.

Audit Rights

Audit rights are of vital importance for the customer, and the cloud provider should be required to grant the customer extensive audit rights, particularly with regard to data security. While a provider may be somewhat reluctant to extend blanket audit rights or insist upon a narrow scope of those rights, data security carries enough importance that a customer should heavily negotiate these provisions. Just a few of the concerns a customer may have that would be

revealed in an audit include, the provider storing the customer's data in cloud locations across the globe, transferring data between various locations without prior notice to the customer, or using parallel storage of data for a multitude of customers on the same servers (which, in some instances, may even be competitors).

Contractual Constellations

As the foregoing establishes, a customer may be best served if it sources the cloud services from a single provider as opposed to several independent providers. However, such cloud providers only provide the cloud itself and do not transfer the data to the cloud. The customer must therefore negotiate the data transfer in a separate agreement with its carrier. In order to ensure that the cloud provider can fulfill its obligations properly, and to avoid unnecessary complications, the customer should aim to find a carrier that is able to provide the bandwidth necessary for the transfer of data envisaged in the agreement with the cloud provider. The service levels of the two agreements should correspond to each other.

In light of this background, a cloud provider's ability to offer additional carrier services, whether itself or through a sub-contractor, could be a unique selling point.

Type of Contract

German law "recognizes" certain types of obligatory agreements that are individually codified in the German Civil Code. Examples of these include lease agreements, work agreements or contracts of sale. These codified agreements or contracts are not conclusive, though. There can also be mixed or hybrid type-agreements, as well as contracts "sui generis." Depending on the type of contract, the legal consequences, such as warranties, possibilities of termination and even the actual obligations, vary. Yet, even in the case of mixed or hybrid agreements, the consequences will often be determined by identifying the legal character of the main component of the agreement. Although this is not a universally binding rule, it's a relatively reliable guide.

Cloud computing contracts are likely to fall into this category of mixed or hybrid agreements, as they often contain several different services and obligations all under a single *roof*, ranging from the provision of services to the hosting and maintenance of data. There may also be a lease component for the storage space or a professional services element in case customization and development is required to make specific software tailored to meet the customer's needs.

Many of these agreements will also place heavy emphasis on the leasing/licensing of software—the backbone of the cloud. Both parties also need to be aware of the peculiarities of lease agreements under German law, which include an express obligation for a lessor to maintain the leased object in a condition suitable for its purposes. This implies a warranty obligation for the duration of the agreement (*i.e.*, the cloud provider has to remedy defects during that period). However, this obligation does not require or stipulate a certain level of performance, rather only that the cloud and its services are maintained in the state upon which both parties have agreed. Service levels, including response times, downtimes, availability and other parameters, need to be determined in the agreement, typically in schedules to the framework agreement.

Back-to-Back Agreements

Some cloud providers are able to provide their services without having to involve third parties such as sub-contractors. In our experience to date, however, the majority of German cloud service providers are relying on sub-suppliers. These providers will need to agree on so-called *back-to-back agreements*.

The expression "back-to-back agreements" implies that cloud providers, as the party directly responsible to the customer, should pass not only the commercial and technical issues for which they are responsible to the sub-contractors, but also the legal issues, in particular exposure to liability. If it does not do so, the cloud provider may find itself in a situation where it is liable to the customer for certain malfunctions or damages that are, in fact, the sub-contractor's responsibility, and the provider will have no recourse to relay these costs to the sub-contractor.

Experience shows that in practice, back-to-back agreements often are not concluded until the "main" contract between the service provider and the customer has been finalized. At this stage, the sub-contractor is in many cases not willing to accept the risks of the service provider. Thus, the cloud provider should conduct parallel negotiations with both the customer and its sub-contractor(s).

Copyright, Indemnification and Licensing Issues

With regard to copyright issues, the cloud provider should make sure that it is entitled to use the software in the cloud for its intended purposes. This is typically not a problem where the cloud provider owns the intellectual property rights to the software, as the customer will receive a license to such technology, subject to appropriate restrictions on use. From the customer's perspective, it

should ensure the cloud provider agreement includes sufficient rights, representations and warranties to use the software in all territories where the customer is likely to do business.

A greater challenge arises in connection with proprietary software of a third party or open source software. Traditional third-party software licensing policies would restrict a cloud provider from making the software available as part of a service free of the typical restrictions. Therefore, these cloud providers must ensure that they have secured modified rights from the third-party licensors.

Further, as a general rule, cloud providers require indemnities against any claim that is made against them as a result of any information, data or electronic material that a customer places in its cloud that causes it to breach a third-party's IP rights, or violates other rights, be it a third-party's personal rights, or regulatory or criminal requirements and prohibitions. Customers should be prepared to offer these concessions.

Data Protection and Data Security

As cloud computing transcends national borders, one of the major areas of concern arises from compliance with German and European data protection laws. Data security must be a crucial issue in any company's data security analysis.

It can be assumed that cloud computing generally involves the collection and use of personal data. Depending on the exact scope of the services, the parties must assess whether the Telemedia Act (Telemediengesetz, the "TMG") and/or the Federal Data Protection Act (Bundesdatenschutzgesetz, the "DPA") applies. While the DPA is the primary legislation regulating the collection and use of personal data, the TMG governs all electronic information and communication services except pure telecommunication and broadcasting (so-called "Telemedia Services"; *e.g.*, web shops, mobile commerce, newsgroups, music download platforms, video on demand, but not live-streaming of video, web-casting, IPTV or VoIP).

At the core of German data protection laws is the requirement that the party (data controller) that decides the purposes for which any personal data is held or processed, and the manner in which it is held or processed, has sole responsibility for safeguarding the data. This includes ensuring that the data controller retains such data under its close control even when the same data is processed by a third party. Understandably, the requirement distinction does not fit easily into the cloud model.

According to German law, data processing by a third party on behalf of the data controller is explicitly regulated in the DPA (section 11, DPA). It requires a written agreement between the data controller and the data processor that describes the agreed data processing services in detail, and must contain certain specifics, which are *inter alia*:

- The technical and organizational data security measures employed by the third-party data processor; this includes by means of law that the customer/data controller is not simply obligated to question and investigate these measures, but is also to effectively check whether the measures are in place and work properly
- Information on the correction, deletion and blocking of data
- Potential sub-processing, if applicable, and allowing for respective arrangements with sub-processors
- Control rights of the data controller and corresponding co-operation duties of the data processor
- Return of data and deletion of data at the data processor's premises

However, inherent in using a cloud provider as a data processor is the loss of control over the processing of data when compared with using a hosted data centre. This causes some conflict with the restriction in German and European legislation on the international transfer of personal data. Data transfers outside Germany must pass two tests:

- Any data transfer constitutes the processing of personal data and requires the consent of the individual whose data is being transferred unless statutory permission exists
- Data transfers outside the EEA are prohibited if the data subject has a legitimate interest in the prevention of the data transfer (sections 4b(1) and (2), DPA). Such legitimate interest is statutorily assumed if and where the recipient does not provide for a level of protection adequate to the protection in the EEA.

In particular, the European Commission has made findings that the United States does not offer an adequate level of protection. Data transfer to a recipient in the United States is therefore permitted only if additional requirements (*e.g.*, compliance with Safe Harbor principles or conclusion of a model contract) are met.

This issue is not merely academic, as these restrictions directly conflict with one of the central efficiencies of operating in the cloud, namely, that the provider can seamlessly move its customers' data between and among its global network of server banks.

German data protection laws also impose a duty on cloud customers to ensure their data processors hold personal data securely. According to the law, this includes the obligation that a customer, as data controller, visits the processor's (*i.e.*, cloud provider's) premises to ascertain whether the required security measures are in place. While it is highly impractical for the German customer (or any customer for that matter) to visit all server locations of the cloud provider for verification of the security measures, this is in theory the requirement imposed by the law. So far, there has been little guidance or comment from the German national data protection authorities on how cloud computing fits within the existing data protection laws and what, if any, particular security measures should be taken.

Cloud providers (as any click-wrap agreement licensor) typically place broad exclusions of liability in their terms of service and do not guarantee compliance with national data protection laws. Companies with strong personal data ties or that regularly collect, aggregate and process (or have processed) other highly sensitive forms of data, in particular, should carefully consider if and how best to transition their business functions into the cloud.

Confidentiality

Data confidentiality is of vital importance to every company across all industries, especially when data sits in the hands of third-party sub-contractors of any kind. Not only must the cloud provider, itself, maintain confidentiality of its customers' data, but it must also extend this obligation to each of its sub-contractors. Providers must also ensure that sufficient transparency exists to allow a customer to review the measures implemented to maintain such confidentiality. The latter point will be difficult to accomplish, though, as the cloud provider will not always agree to provide the necessary insight and transparency to its customers.

Legal Enforcement

An important point to be taken into consideration is the difficulty a customer may face in enforcing its potential claims against a cloud provider. It is commonplace in the IT business to discontinue certain services, amend/modify software or hardware, or relocate customers to other services that are more economically efficient for the service provider. All of these actions could possibly result in disastrous situations for the customer who has relied on the availability of the services and the outplaced data. In theory, the agreement should provide for a multitude of legal remedies to cover these situations. However, even if German law is applicable and the German customer is able to push for a German venue, the legal remedies are usually not sufficient to ensure immediate assistance for a customer. Even the swiftest form of a legal remedy, a preliminary injunction, will generally take a few days to obtain. That can be too long a period when a customer needs to access to data and/or when a customer's business has been severely impeded. A proceeding on the merits can only serve as a retrospective appraisal of the situation and an assessment of warranty or damage claims.

If the cloud provider is not in Germany, and applicable law and venue are also outside Germany, the possibilities of legal enforcement for a German customer will diminish even further.

Summary

In Germany, cloud computing is still in its infancy. Many of the major providers are currently trying to identify their principal markets, thus reflected in many of the loose service descriptions and relatively generic terms that have been batted around as of late. However, regardless of a number of open technical and legal issues, consulting firms recommend dealing with cloud computing, and at least recommend experimenting with cloud computing in order not to miss out on a very promising technical trend.

— Biographies of Authors and Editors —

Thomas Fischl, Counsel – Munich +49 (0)89 20304 178 jfischl@reedsmith.com

Thomas is counsel in the European Corporate Group in Munich and part of the Media & Technology Team. He provides comprehensive legal advice to mid-sized and major IT providers and companies in both the domestic and international markets, within the scope of IT law. His particular experience covers drafting and negotiating contracts covering software, IT projects, and distribution, as well as outsourcing projects. In addition, Thomas specializes in data protection law and intellectual property protection. He also serves as legal counsel in project crises and asserts his clients' interests in court. His clients include not only software and technology companies, but also clients from such industries as mechanical engineering, automotive, marketing, financial services and health care.

Katharina A. Weimer, Associate – Munich +49 (0)89 20304 160 kweimer@reedsmith.com

Katharina is a member of the European Corporate Group and specialises in the area of Advertising Technology & Media (ATM). She is a commercial lawyer with a strong focus on all media- and entertainment-related matters. Among her clients are international broadcasters as well as new and old media enterprises. She also has substantial experience in copyright-related contentious and non-contentious matters, international and national data protection matters, and all aspects of doing business on the Internet. Katharina's main focus is supplemented by continuous advice in life sciences and clinical trial projects, involvement in various international transactions and litigation, and extensive experience in agreements for the virtual world.

— Cloud Computing Task Force Leader —

Joseph I. Rosenbaum, Partner and Chair, Advertising Technology & Media Law Group
New York · +1 212 702 1303 · jrosenbaum@reedsmith.com
Blog: www.LegalBytes.com

Joe is a member of Reed Smith's global Advertising Technology & Media Law practice, and has more than 30 years of international experience across a wide range of sophisticated and complex commercial transactions, in industries including advertising, entertainment and media, financial services, travel-related services, technology and many more. Joe specializes in the law and policy arising at the intersection of technology and online and behavioral advertising, social media, entertainment, finance, e-commerce, information security and digital rights, online gaming, promotions, privacy and data protection, among others. Joe's experience includes virtual worlds, mobile marketing, digital payments and PCI compliance, digital broadcasting, co-branded credit and gift cards, loyalty rewards programs, branded entertainment, online product placement and endorsements, user-generated content, buzz, word-of-mouth and viral marketing, licensing, software development and outsourcing. Joe lectures and writes extensively and, among others, has authored a book on outsourcing (*Outsourcing Agreements Line by Line*; Aspatore Publishing, 2004) and a seminal law journal article on privacy ("Privacy on the Internet: Whose Information Is It Anyway?"; *Jurimetrics Law Journal*, 1998). Joe's work has been cited by appellate courts, law reviews and journals, industry and trade periodicals. Joe is regularly quoted in widely respected publications such as the *National Law Journal*, Advertising Age, the American Banker, Euromoney and has been interviewed and appeared as a commentator on CNBC's *Squawkbox* and CNN Financial's *Business Unusual*. Joe is General Counsel & Secretary to the Interactive Advertising Bureau and a member of the Advisory Board of the Center for Law, Science and Technology at the Sandra Day O'Connor College of Law at ASU.