Published on *Telsoc* (https://telsoc.org)

Navigating a cloud services agreement

Lars Perhard [1]

Cloud Sweden Legal Group

AJTDE - Vol 1, No 1 - October 2013 [2]

[3]

★ 42 [4]

Abstract

Cloud Sweden is a story about how a group of experienced IT-people from different sectors of the industry came together and discussed a relatively new phenomenon called the Cloud; or what is today labelled as Cloud computing. And they realised there was a tremendous momentum and potential prosperity connected to it. They also concluded that in order to support potential users and to promote Sweden as an IT-oriented country in the forefront of the development there was a need for information ? organisations considering migrating their IT functions to the Cloud should at least be able to make an informed decision. There are significant advantages with this new technology, but also a number of pitfalls that any user should be aware of. There were for example critical security issues at hand before when the servers were placed within the four walls of the office and there still are critical security issues relating to the Cloud. However, the issues to solve are different. Cloud Sweden was founded and the different branches of the group have produced a number of documents published on its website. Cloud Sweden has apart from a number of members working actively in the steering and competence groups several thousand members from the industry in a Linkedin network. In this article you will find a sample of what the legal group of Cloud Sweden has produced ? a primer of legal issues that a migrant shall pay attention to before the leap into the Cloud.

Introduction

Cloud Sweden was founded nearly two years ago by a group of enthusiastic members of the Swedish Data Society (Sw. Dataf?reningen), and is now a non-profit working branch and network within the Society. Moreover, Cloud Sweden has become the independent focal point for Swedish expertise on Cloud services. Cloud Sweden promotes safe and appropriate usage of Cloud services, and endeavours to make Sweden one of the world leading nations within the area. Cloud Sweden also aims to contribute to international competence developments within the Cloud.

Cloud Sweden is working on developing criteria for secure Cloud services. This is done from a technology, legal, operational and security perspective, where the user?s interests are central.

The organisation works broadly to create and make available qualitative information. Cloud Sweden is open to anyone who wishes to get involved. All material within the organisation is developed under the Creative Commons Licence 3.0 Attribution-Share-Alike. It means, simply, that the material published can be used provided the source is acknowledged and provided any adaptation of the material is made available under the same licence.

Soon after the outset of its foundation Cloud Sweden also formed a legal group that started to analyse the legal aspects of Cloud services. The legal group has had more than twenty active members consisting mainly of IT-lawyers and scholars. So far the legal group has been very productive and has published a number of useful documents on its website[i] [5]. The group has developed a primer or a first legal checklist, but also several other documents that should be helpful to those considering a migration to the Cloud. The group has *inter alia* produced

1. a memo that addresses special aspects to consider when applying Cloud technology in the public sector, [ii] [6]
2. a report that analyses unreasonably pro-supplier terms and conditions for Cloud services issued by the Swedish Federation for IT & Telecom Corporations (IT & Telekomf?retagen)[iii] [7] and has also
3. a basic checklist covering basic tax issues relating to both domestic and cross-border Cloud sourcing projects.

This article aims to sum up some of the fundamental legal aspects of Cloud services that a potential organisation should consider before deciding to migrate its IT-operations to the Cloud; the information has been taken from Cloud Sweden?s checklist addressing the same. The checklist can be found on Cloud Sweden?s site as above.

Cloud Sweden has found this approach of particular interest, as Cloud services at first glance often seem to be extremely attractive because of their competitive and favourable low cost model. The information in the legal group?s checklist has been tailored firstly to fit small and mid-size businesses and organisations and their management and not necessarily full-fledged in-house or external counsel.

Legal challenges

In the legal analysis, it is first necessary to investigate whether any legal obstacles to the use of Cloud services exist. In practice, e.g. from a Swedish perspective as in many other jurisdictions, there are few direct legal challenges, but sometimes requirements set forth in legislation may be difficult to fulfil using Cloud services. Such obstacles are often related to specific security requirements for a given activity or for a particular type of information. More common, however, is that general legal requirements for security, e.g. confidentiality, security in the processing of personal data[iv] [8], stock exchange requirements, need to be converted to requirements set out when choosing a Cloud service provider or to security requirements in the contract for Cloud services. With an increased flow of business secrets that are sent and placed outside corporate firewalls, the encryption of data must also be considered.

Information security

Cloud Sweden also has a working group focusing on security issues only, but more from a technical perspective. These issues often go hand in hand with the legal issues, as all aspects of security should be addressed in a Cloud sourcing agreement. A migration of services to the Cloud places special demands on the systematic work of information security ? not only on the supplier but also on the customer. Deficiencies regarding information security that already exist at the customer?s end before any decision is made to use Cloud services will not automatically be corrected through migration. In most cases, it will instead become more complex to address the shortcomings when the services are placed in a Cloud environment. Used in the correct way, however, Cloud services can in most cases provide an adequate level of security.

Due diligence

A general observation is of course, as in so many other types of business transactions, that a customer should not rely entirely on a well-designed contract, but should also investigate the status and history of a supplier. This can, for example, involve obtaining references or carrying out a more or less comprehensive survey of the supplier?s operations and status, from a legal, financial and technical perspective (due diligence), where the customer may for example have access to the supplier?s documentation, routines and processes in order to determine the supplier?s ability to meet the customer?s requirements.

These aspects are particularly important as Cloud services in most cases are delivered by players in the international arena. For small or mid-size organisations it can become too costly to initiate legal proceedings abroad in the event the supplier does not fulfil its commitments. Therefore, it can sometimes be of the essence for a small player to hire a cloud supplier that is well-known for being careful with its reputation, and also to be ready to migrate to another supplier should the services not be price-worthy.

International aspects

Cloud services are often performed across borders and in different parts of the world simultaneously. Thus, it is not sufficient simply to find out where data is stored, but also where it is processed in the case that Cloud services are used for the processing of data, since providers often try to optimise their computing power when processing data. This means that information can be transferred for the purposes of processing, and then returned and stored in processed form at the agreed storage site. The consequence is that a customer ? regardless of what the contract says ? may be exposed to the legal systems of other countries. These technical aspects are important in determining how, for example, personal data protection issues are solved (see below). Moreover, data stored within a particular country can, for example, be subject to publishing laws or the equivalent, or forcibly made available to [local] authorities such as police or intelligence agencies.[v] [9] Such circumstances should also be considered before Cloud services are used.

Risk analysis

Before a decision on transition to the Cloud is taken, the customer must analyse the applicable risks and requirements in the given situation. It is essential that the customer converts the results of the analysis to precautionary measures and communicates these to the provider. Cloud Security Alliance has identified a number of primary threats to deal with in connection with a migration to the cloud.[vi] [10] Some of all the features elaborated on will be found below:

- Secure transfer of data in the cloud
- Secure storage
- Secure access to the services
- Secure deletion of data
- Compromised data
- Define the level of data protection.

General contractual issues

Providers generally present their own standard terms and conditions as a basis for Cloud service contracts. The proposed contract terms are often favourable to the supplier. A prospective customer should therefore familiarise themselves fully with the terms that are offered. The fact that Cloud services are largely standardised by the suppliers means that room for individual contract negotiation is often severely limited. In such situations, it is important that the customer carefully examines different providers? standard terms before choosing a provider[vii] [11]. The scope of the business or the relationship between the parties may mean that the customer is in a better position to individually negotiate terms of the Cloud service contract, for example, if the contract is being entered into with a local provider of Cloud services who provides some customer-specific adaptations.

Service specification is crucial for what a customer can require from the Cloud service. It is important that the customer ensures that the specification corresponds to the needs of the business. The customer should ensure that the specification is clear enough so that it can easily be determined if the provided service is in accordance with the contract or not. Additionally, it should clearly be stated what requirements the use of the Cloud service places on the customer?s operating environment.

A customer should avoid accepting that some contractual issues shall be determined and resolved after the signing of the contract, but in such a case the contract should include provisions on how this will be done and what will happen if the parties fail to agree. The customer should pay particular attention to contract terms that give the supplier the right to unilaterally change the service specification[viii] [12]. It should be considered whether the customer will be given the right to approve, in advance, all the supplier?s subcontractors that will process or otherwise come into contact with the customer?s data. The contract should clearly state the requirements that must be met by the provider if and when the contract ends.

Personal data legislation

An example of a legal framework that applies for every use of Cloud services is personal data legislation. Users of Cloud services need to be aware of the responsibilities arising from the provisions of the [Swedish] *Data Protection Act*. This means, amongst other things, that the Act?s rules on when processing of personal data is permitted must be taken into account, that the Act?s security requirements must be met and that there must be an agreement that regulates the Cloud service provider?s processing of personal data. In order for personal data to be included in a Cloud service whereby data may be stored outside the European Economic Area (EEA) (i.e. EU and EFTA countries), specific legal requirements apply. Anyone who wants to use a Cloud service for storing personal data must therefore either ensure that storage occurs only within the EEA or actively ensure that they meet the requirements for transfer to a third country.

Cloud services are often carried out across borders and in different parts of the world simultaneously etc. From the perspective of personal data legislation, however, the transfer for the purposes of processing, the processing itself and the returning of the processed data are all processing of personal data. The contract should clearly state where the customer?s data may be processed (for example determined to a region, country/countries or data centres) and that this processing is traceable. Where systems? administrative work may be carried out should also be covered in the contract.

The contract should, as a minimum, include the provisions that according to the *Personal Data Act* should be found in a contract with a party who processes data on behalf of the customer. Also ensure control over where and by whom personal data is processed. For example, the customer should consider including provisions that the provider shall assist the customer in questions concerning obligations under the *Personal Data Act*, that consent should always be obtained from the customer in the case of the use of a subcontractor or if personal data shall be transferred to a third country (i.e. countries outside the EEA), that the provider shall bear the costs and risks relating to agreements with subcontractors and that the provider will reimburse the customer for any damage caused to the customer due to the supplier or subcontractor failing to meet obligations arising from the contract.

If the contract allows the Cloud service provider in practice, directly or indirectly through subcontractors, to process the customer?s personal data outside the EEA, the contract must include regulation of the legal basis for this. There are several ways in which the customer can ensure that requirements for the transfer of personal data to a third country are met. The customer can, for example, conclude a separate standard contract[ix] [13] (a so-called ?model clause contract?) with the provider that regulates the transfer of personal data. Here it is also important to consider what kind of data is being transferred in the particular case, how long the processing will last and what kind of data protection rules exist in the country where the processing wishes to be carried out.[x] [14]

Confidentiality and encryption

Confidentiality is achieved by creating the ability to prevent unauthorised persons from gaining access to one?s own data. In certain circumstances, legal requirements set explicit demands that certain information shall be given confidentiality protection in this way; one of the best examples is the framework of the [Swedish] Official Secrets Act (2009:400). Confidentiality requirements need to be addressed in the contract with the provider of Cloud services. The contract should state that the customer?s data is not allowed to be disclosed to third parties or to be used by the provider for purposes other than the provision of services. The provider should ensure that access to the customer?s data is limited to those persons within the organisation who need access to the data in order to perform their duties.

It should also be regulated how, and in what way, the provider can monitor and collect information about how, and to what extent, the customer uses the service (such as frequency, changes in volume and bandwidth usage etc.). If the provider is given such a possibility, this should be strictly regulated and in addition state which parties (companies, authorities etc.) the provider is able to share such information with.

Particularly sensitive data shall be protected by encryption when transferring to and from the service provider. It should also be considered whether the data should be protected by encryption when in ?rest?. Furthermore, it shall be ensured that the service meets the applicable regulations on export control, particularly in cases where the service is delivered from the USA.

The contract should also include a requirement for the provider to store the customer?s data separate from other customers? data.

Service levels

Depending on whether the service is wholly or partly standardised, it may be necessary to contract on customised service levels. Checklist for negotiating service levels:

1. Start from the customer?s real needs and consider what constitutes appropriate requirements and what should and can be measured regarding the service at hand;
2. Service levels should always be well adapted to the needs of the business as otherwise they can lead to unnecessary costs;
3. In a Cloud service the connection is of a relatively simply nature, which is why other parameters than late delivery should be measured, such as correction times in cases of error, availability and response times;
4. Given that the provider itself controls the design and implementation of the service, the provider?s exemptions from liability should be relatively limited;
5. If the provider states a percentage for availability, this shall be converted into absolute numbers in order to get a precise estimate of, for example, how many minutes per month a service can be down without incurring liability for the provider;
6. Consider whether the whole service requires the same service level or if differentiated levels are a possibility, for example a heightened level of service for specific customer-critical applications or different levels weekday/weekend and day/night;
7. Describe how service levels can be adjusted over time, and how they should be measured and reported.

Penalties

Penalty payments are often given as a sanction when service levels are not met. In case of delays in the customer?s connection or service failures, the customer should be compensated.

Penalties should be calculated on everything the customer cannot use as a result of the failure, and the customer should as a starting point be compensated in full for any potential harm. This means that damages may be awarded in addition to penalty payments if the customer can show that the harm is not covered by the penalty payment. The penalty rates do not need to be the same for the whole service, but can be differentiated e.g. by:

- Different penalties depending on whether or not a particular service is customer-critical.
- Cumulative penalties where repeated events or multiple simultaneous failures.
- Use of greatly increased penalties relating to the most business-critical systems or failures of significant importance.

The customer should always consider whether it is appropriate to impose alternatives or complements to penalties, such as various incentives to ?reward? a provider for the good provision of services, particularly where such a provision contributes to a better result for the customer.

Security (back-up, loss of data etc.)

A fundamental requirement from the customer on the provider should be that work with information security is conducted in accordance with established standards within the field. Adequate security measures must exist, for example in the form of a security policy, access control (including administrative procedures), logging and tracing, procedures for incident management and reporting, malware protection, back-up with periodic inspection of re-readability and continuity planning, and possibilities for security audit of both the customer and of third parties should be regulated in the contract. The structure and level of each security measure should be determined by the result of the customer?s analysis of risks and requirements.

The customer should clarify and match the role of the provider in the customer?s continuity planning with the provider. For example, the customer should consider whether all or part of the service should be covered by alternative infrastructures that create redundancy.

Consider who shall be responsible for *loss of data* (for example due to technical failures, theft of data or intrusion) and how this term is defined in the particular case[xi] [15]. It is important that the contract clarifies precisely what is considered to be included in such a loss, and which party shall bear responsibility for precautionary measures such as resets and back-ups. The customer should therefore critically review the wording of some suppliers, that data loss is considered to be indirect harm, and as such exempt from the responsibility of the provider.

Termination and exit

The contract should include provisions that clarify the obligations of the provider to assist the customer when moving to another provider or back to the customer. The contract should specify in detail the provider?s obligation to assist the customer and cooperate with the new provider; how and when this shall happen and whether the provider in addition to returning data should even destroy or anonymise data that does not return to the customer.

It should also state when these obligations arise ? for example upon termination of the entire contract, part of the contract and/or some specific service. Even where open standards are used it is not simple to migrate data. It is therefore important to regulate the manner and format in which the customer?s data shall be returned in order to avoid lock-in effects. The provider can in principle never have the right to withhold the customer?s data. This should be clearly stated in the contract.

Limitations of liability

Typically, contracts from providers contain different forms of liability limitations. The customer should in each case carefully consider whether and in what ways the provider should be able to limit its liability. Find the balance between, on the one hand, a reasonable limitation of liability, and on the other, the importance of not eroding the provider?s basic responsibility. Such an erosion risks reducing the provider?s incentive to act in accordance with the provisions of the contract. Requirements for an unlimited or very broad responsibility of the provider risk affecting the customer in the form of a price increase.

Often it is better to clearly state what type of damage is to be covered or not covered by a limitation of liability, instead of relying on the traditional division between direct and indirect damages (in Swedish law as well as in many jurisdictions). Consider that a large part of the damage a customer can suffer is in fact in the form of indirect damages, such as lost revenue. An unlimited obligation in this respect creates a large exposure to risk and a lack of predictability for the provider.

Even though it is often reasonable that the provider in some way limits their liability, it should be mentioned that various possible scenarios should be considered, taking account of the risks envisaged by the customer in the particular case. If it is reasonable to require that the provider take some responsibility even for indirect harm, exposure can for example be limited through a specified ceiling for compensation.[xii] [16]

Force Majeure

Adapt the force majeure clause to the specific case. If the provider chooses an offshore alternative, where parts of the provider?s operations, such as storage, are placed in a country with a completely different infrastructure, climate conditions and so forth, a *force majeure* clause, and what is to be considered an ?unforeseen event?, should be interpreted in view of this.

For Cloud services where the customer connects to a service supplied by the provider only via the Internet, for example, the provider has full control over the whole process. All material from the customer ends up with the provider, where the customer?s involvement and contacts are much less than they have traditionally been in IT-delivery. The provider itself determines the quality of servers and other equipment, along with procedures for back-ups, redundancy, etc. This should mean that the provider of these new Cloud services would be able to take a larger and better-defined responsibility in terms of data loss than previously. Avoid any requirement that the customer has the burden of proof in demonstrating the emergence of a fault and its nature.

Intellectual property rights

The provider should guarantee the necessary intellectual property rights for the service and assume responsibility that the use of the service will not infringe third party rights. It is not uncommon that licence terms are country-specific, so the customer should ensure that the use of the service is guaranteed in all countries where the customer operates. At the same time, one of the benefits of Cloud services are that they are available ?everywhere?, so a global guarantee is of course preferable. In the case that the contract for example includes infrastructure or platforms, the customer should ensure that the customer?s licence agreement allows for use in such an environment.

Clarify that the customer unlimitedly owns and shall retain all rights to its data and that the customer?s rights cannot be transferred to the provider. The definition of ?customer data? in the contract should include data that the customer uploads to the provider, and the result of the provider?s processing of data.

Termination of service

A customer is completely dependent that a Cloud service is continuously delivered; any potential ability for the provider to terminate the service should therefore be regulated in detail. It is important that the contract states in detail when such a possibility of termination shall exist. The provider should not have the right to terminate the service at its discretion. For a customer, it is often reasonable to require that the service may not be terminated without a decision of a court or arbitration tribunal, or if there is a serious and real risk to the security of the provider, or if the service is being used to commit crime. An allegation of a breach of contract by the customer, for example, should not be the basis for termination of service. The contract should also include provisions on the obligation for the provider to keep the customer?s data for a certain time even if it is proven that the provider has the right to terminate the service. The time period should be sufficient for the customer to recover its data.

Flexibility, changes of service and reporting

In cases of new forms of cooperation that are developing it may be difficult initially to anticipate situations that may arise or how these should be resolved. As Cloud services involve a new form of cooperation for both customer and provider, the contract should be flexible and include regulations on how changes are handled. In Cloud services where the provider has control of the customer?s data and where the customer is unable to inspect how the provider carries out its service, collaboration and reporting should have prominent roles. It is important that the contract stipulates that the customer?s and provider?s respective IT-incident management organisations shall work closely together. How cooperation and reporting will occur should be specified. The customer should receive regular status updates, information on incidents that have occurred, etc. Important issues should be handled in a continuous and open dialogue (for example concerning security), and the collaboration levels where decisions can be made shall be indicated. The ability to escalate, at an early stage, key issues that arise should be addressed . To avoid future discussions, meeting minutes should always be kept and approved by both parties.

A characteristic feature of Cloud services is flexibility and ease of ordering. There is thus a risk/possibility that the customer?s organisation enters into a decentralised and uncontrolled IT-procurement. If the customer experiences such decentralisation as negative, the permission to place orders and even the amount and types of service should be regulated in the contract. This maintains the customer?s IT or sourcing department?s control.

Use of customer data for purposes other than the provision of services

There are Cloud providers who want to use customers? data for themselves, i.e. in addition to providing the service to the customer. This can of course be for legitimate reasons such as where the provider uses aggregated data in order to learn more about the needs of its customers and thereby acquire knowledge to be able to improve the service. A reasonable basic assumption is, however, that the customer does not want anyone else using the customer?s data. The customer should therefore ensure that the contract is in fact in line with the customer?s understanding on this issue. To the extent that the provider processes the customer?s personal data for uses other than the provision of services back to the customer, the provider becomes the data controller. If the customer allows the provider to process customer data for purposes other than the provision of services back to the customer, this discretion must be clearly specified in the contract.

Jurisdiction and choice of law and forum for dispute resolution

Applicable law

The question of applicable law is related to the type of situation that is at hand. For example, criminal issues are usually determined according to the law where the alleged crime was committed; data protection issues are assessed according to the law of the country in which the data controller resides, but other jurisdictions may come into play depending on where the personal data is processed. There are therefore a number of situations where the contracting parties do not have at their disposal the choice of applicable law.

The contractual relationship

For contractual relationships between the parties, for example in situations where one party wants legal sanctions against the other party, the country?s law in which the contract is most associated often comes into play. Within the EU the so-called Rome I Regulation on contractual obligations[xiii] [17], amongst others, applies. The basis of the conflict of law rules in the Regulation is that the contracting parties themselves can decide which country?s law applies to the contract. If the parties have not agreed on this, the general rule is that the laws in the country with which the contract is most closely connected shall apply. This connected country is normally the country in which the party who, according to the contract, shall carry out a performance has its residence. In a cross-border Cloud service contract this should in general be the service provider?s country. If one of the parties is located outside of the EU, the situation becomes more complicated.[xiv] [18] It is therefore recommended in contracts for cross-border Cloud services that the parties always decide upon the applicable law in the contract. In the case where e.g. a Swedish party has been forced to accept a foreign legal system, there may be grounds for consulting a lawyer in that country in order to clarify the consequences of the various provisions of the contract.

The provider?s standard terms and conditions typically state that a dispute shall be decided according the law of the country where the provider is established. The customer should not, without further analysis, accept such a provision. A Cloud service contract should, taking into account that mentioned above, contain a provision governing which country?s law should be applied if a dispute between the parties arises.

Forum ? court

In contracts involving cross-border relationships, it may also be important to clarify in the contract where and in which country a dispute shall be resolved. In the EU (Brussels I Regulation) the parties have in principle the right to choose the court that shall hear the case. Otherwise, the general rule is that proceedings shall be brought in the defendant?s country of residence; an exception is, for example, that for breach of contract the case shall be heard in ?the place of performance?, i.e. the place where the Cloud services should have been provided. A disadvantage with the court process is that it can take a relatively long time - compared to the arbitration procedure ? for example because there are possibilities to appeal. In cross-border disputes that extend beyond the EU, the court process is less appropriate for several reasons. Amongst other things, it is often hard to get a court judgment enforced in such a country.

Arbitration

Arbitration as a dispute resolution model is particularly interesting in terms of Cloud services, as an arbitrary award is in principle enforceable in most countries, according to the New York Convention (from 1958)[xv] [19].

The contracting parties can, by including an arbitration clause in the contract, choose to resolve any disputes out of court. The process is voluntary, but is regulated by law. The parties can even choose that the arbitration proceedings shall be confidential, and that the proceedings be adapted to the needs of the parties in a number of ways. Firstly, the parties themselves have the opportunity to appoint their arbitrators, who in turn jointly appoint a chairman; secondly they have the possibility to choose arbitrators with the right expertise. An arbitrary award is in principle not appealable. At arbitration, while the parties pay the tribunal or arbitrator, the costs for representation are often high. Legal proceedings that can lead to trial in more than one instance risk generating substantially higher representation costs. Responsibility for costs is in principle the same general rule as in court, i.e. the unsuccessful party bears its own costs for the proceedings, along with those of the other party.

The Stockholm Chamber of Commerce Arbitration Institute (SCC) provides extensive information about arbitration and its rules on the website www.sccinstitute.se [20] where various types of model clauses can be found[xvi] [21]. For smaller projects, the parties can choose a so-called facilitated arbitration procedure that can be carried out relatively quickly at a limited cost. In such cases only one single arbitrator is appointed.

An arbitration procedure under the SCC?s rules may also be preferable as the arbitration rules that have been developed provide more extensive guidance than that provided by law for how the process shall proceed. There may be good reasons to enlist the help of a knowledgeable lawyer in order to inform one?s self about the pros and cons of various dispute resolution models.

Endnotes

i [22] See www.cloudsweden.se [23]; however only some material is available in English
ii [24] Sweden is in the forefront of the development. Increasing numbers of municipalities, authorities and businesses are considering the use of so-called cloud services
iii [25] Swedish IT and Telecom Industries is a member organisation for companies of all sizes within the entire IT and telecom sector, that wish to join the largest industry network in Sweden in order to promote and further develop the IT market and conditions for IT enterprises. The organisation has developed a standard agreement for Cloud services which can be bought on their web-site: http://www.itotelekomforetagen.se/standardavtal/vara-standardavtal [26]
iv [27] The EC Directive on data protection requires that all member states have rules that provide an equivalent protection for personal data and privacy, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT [28] . EU as well as Sweden as a member state can be considered to have a high standard concering the protection of personal data. The EC-directive has been implemented in Sweden and here you can find the Act in English: http://www.government.se/content/1/c6/01/55/42/b451922d.pdf [29]
v [30] One shall not go into the ?Snowden debate? here.
vi [31] Cf. https://cloudsecurityalliance.org/ [32]. Here the reader will be able to find an extensive elaboration of all the risks.

vii [33] This article does not aim at consumer rights However, even a business enterprise might refer to the e.g British *Unfair Contract Terms Act 1977* in rather serious cases. From a Swedish perspective Section 36 of our Contract Act could possibly have an unconscionable condition set aside in a cloud contract. However, as mentioned above it might not be feasible to access justice for a small player vs a strong supplier.
viii [34] When it comes to consumer-related cloud services offered for free it might be considered reasonable that terms & conditions can be amended only by one party/the supplier. However, this feature has sometimes been tried by cloud suppliers in B2B situations. A basic rule in Sweden, as well as in many other civilised jurisdictions, is that it shall be deemed impossible or at least unconscionable to change a contract through an action of only one party (the old principle *pacta sunt servanda* is still prevailing in Swedish law*).*
ix [35] Model Contracts for the transfer of personal data to third countries, cf. http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm [36]
x [37] The provider may be responsible for personal data if it processes the customer?s data beyond the scope of the purpose of the service. An extremely interesting and valuable analysis has been med by Queen Mary University in 'Negotiating Cloud Contracts ? Looking at Clouds from Both Sides'. Now, cf. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055199 [38]
xi [39] Loss of data could be due to e.g. human error - accidental or unknowing data deletion, modification, overwrite; File corruption ? software error, virus infection; Hardware ? drive failure, controller failure, CPU failure; or Site-related ? theft, fire, flood, earthquake, lightning, etc. Cf. http://www.bostoncomputing.net/consultation/databackup/dataloss/ [40] It is of interest to elaborate on these factors to see to what extent they are relevant in a cloud computing context.
xii [41] In the Queen Mary report, cf. above, there are a number of examples from contractual situations, e.g. one where some SaaS providers emphasised that they provide services rather than licensing software and wished to limit liability to a minimum.
xiii [42] Regulation (EC) No 593/2008 [43] of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) cf. http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/jl0006_en.htm [44]
xiv [45] To the extent there is no international convention applicable. The parties will have to rely on rules in inter?national private law, that is in practice the rules in each jurisdiction which decides on which elements of a contract that shall apply to foreign law, and if that is case, which foreign law shall be applicable. Basically, in *hands on perspective* an Australian court will apply Australian international private law and a Swedish court Swedish International Private law.

Just a simple example concerning the validity of a will and the power to make a will at a certain point in time. Under Swedish international private law (codified) the rules of the law of the country in which the testator/testatrix was citizen at the time the will was made shall be applicable. When it comes to the contractual parts of a cloud sourcing agreement many jurisdictions will tend to look at the issue which party is performing the most and that gives overweight to the country of the supplier. However, each particular case will have to be analysed. In international arbitration a conflict between different national laws will be solved by the arbitral tribunal from the viewpoint of the laws where the arbitration has its seat.
xv [46] English Text of the New York Convention [47]: 1958 - Convention on the Recognition and Enforcement of Foreign Arbitral Awards - the "New York" Convention: http://www.newyorkconvention.org/texts [48]
xvi [49] An arbitration can only take place if there is an arbitration agreement between the parties. SCC recommends that a dispute resolution clause is included in any business agreement. The dispute resolution clause shall state the manner in which any dispute between the parties shall be solved. Where the parties agree to arbitrate any disputes under the SCC Rules, it is recommend that the SCC Model Clauses are included in the contract. The Model Clauses can be found in a number of variations to suit the parties' wishes; clauses referring to the Arbitration Rules or the Rules for Expedited Arbitrations only, and various combination clauses giving greater flexibility when the size and character of any dispute is more difficult to predict. Cf. http://www.sccinstitute.com/?id=23710 [50]
Article PDF:
ajtde_2013_1_1_08-perhard.pdf [51]

Cite this article as:

Lars Perhard. 2013. *Navigating a cloud services agreement*. ajtde, Vol 1, No 1, Article 8. http://doi.org/10.18080/ajtde.v1n1.8 [53]. Published by Telecommunications Association Inc. ABN 34 732 327 053. https://telsoc.org [54]

Legal issues in cloud computing [55]
security in cloud computing [56]
Cloud computing [57]
cyber attacks [58]
Cloud computing [57]
privacy in cloud computing [59]

Source URL: https://telsoc.org/journal/ajtde-v1-n1/a8

Links

[1] https://telsoc.org/journal/author/lars-perhard
[2] https://telsoc.org/journal/ajtde-v1-n1
[3] https://www.addtoany.com/share#url=https%3A%2F%2Ftelsoc.org%2Fjournal%2Fajtde-v1-n1%2Fa8&amp;title=Navigating%20a%20cloud%20services%20agreement
[4] https://telsoc.org/printpdf/286?rate=O7Es-_TxTjyW1O-TPkQksHaYiZQ8sX46nhK6GxnxhTg
[5] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote1sym
[6] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote2sym
[7] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote3sym
[8] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote4sym
[9] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote5sym
[10] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote6sym
[11] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote7sym
[12] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote8sym
[13] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote9sym
[14] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote10sym
[15] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote11sym
[16] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote12sym
[17] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote13sym
[18] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote14sym
[19] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote15sym
[20] http://www.sccinstitute.se/
[21] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote16sym
[22] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote1anc
[23] http://www.cloudsweden.se/
[24] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote2anc
[25] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote3anc
[26] http://www.itotelekomforetagen.se/standardavtal/vara-standardavtal
[27] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote4anc
[28] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT
[29] http://www.government.se/content/1/c6/01/55/42/b451922d.pdf
[30] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote5anc

[31] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote6anc
[32] https://cloudsecurityalliance.org/
[33] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote7anc
[34] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote8anc
[35] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote9anc
[36] http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm
[37] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote10anc
[38] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055199
[39] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote11anc
[40] http://www.bostoncomputing.net/consultation/databackup/dataloss/
[41] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote12anc
[42] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote13anc
[43] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008R0593:EN:NOT
[44] http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_civil_matters/jl0006_en.htm
[45] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote14anc
[46] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote15anc
[47] https://telsoc.org/../../userfiles/documenten/nyc-texts/21_english.pdf
[48] http://www.newyorkconvention.org/texts
[49] https://telsoc.org/journal/ajtde-v1-n1/a8#sdendnote16anc
[50] http://www.sccinstitute.com/?id=23710
[51] https://telsoc.org/sites/default/files/tja/pdf/ajtde_2013_1_1_08-perhard_0.pdf
[52] https://telsoc.org/copyright
[53] http://doi.org/10.18080/ajtde.v1n1.8
[54] https://telsoc.org
[55] https://telsoc.org/topics/legal-issues-cloud-computing
[56] https://telsoc.org/topics/security-cloud-computing
[57] https://telsoc.org/topics/cloud-computing
[58] https://telsoc.org/topics/cyber-attacks
[59] https://telsoc.org/topics/privacy-cloud-computing