LEXOLOGY

At a glance: cloud computing contracts in Sweden

Advokatfirman Delphi

Sweden | November 12 2020

Cloud computing contracts

Types of contract

What forms of cloud computing contract are usually adopted in your jurisdiction, including cloud provider supply chains (if applicable)?

Usually, the supplier's standard cloud computing contract is applied. Given the bargaining power of the customer, the cloud computing contract may, in rare cases, be based on the customer's standard template, in particular, when the supplier is a local cloud provider. Notwithstanding the above, for certain areas of the cloud computing contract, the suppliers, including international cloud providers, have become more recipient towards implementing customer requirements in the contract. This relates, in particular, to regulatory requirements, such as requirements deriving from privacy legislation and regulations, requirements on public sector entities and financial regulations.

Typical terms for governing law

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering governing law, jurisdiction, enforceability and cross-border issues, and dispute resolution?

As cloud computing contracts are often drafted on the basis of the supplier's standard cloud computing contract, governing law will, in many cases, be the law that applies where the supplier's business is based, such as the laws of Ireland or the US. However, you may also find contracts that are governed by Swedish law, in particular from local Swedish cloud suppliers, but also larger international enterprises that have opened up local Swedish entities.

For data privacy, Swedish law will typically apply, in particular since this is a regulatory requirement from the Swedish Data Protection Authority (DPA) or at least that was the case prior to the General Data Protection Regulation (GDPR). As to jurisdiction, principles corresponding with those above would normally apply. In most Swedish B2B contracts, arbitration is used as a method of dispute resolution and this would typically also apply to cloud computing contracts. Ultimately, the choice of rules for dispute resolution as well as governing law and jurisdiction would be the result of the parties' negotiations. Many of the larger cloud service providers will not accept that the agreement will be governed by Swedish law. The enforceability of a cloud service contract is, however, uncertain as there is very limited case law regarding this matter.

Cross-border issues are mostly discussed in respect of data privacy and secrecy. Data privacy cross-border issues are usually regulated through the use of the standard contractual clauses decided by the EU Commission on 5 February 2010 (2010/87/EU) that supplement the cloud computing contract to allow transfer of personal data outside the European Economic Area (EEA). Many cloud service providers are reluctant to provide a guarantee that data will not be processed outside the EU and EEA even if they may commit to mainly using data centres

within the EEA as their main facilities for the services. The newly adopted US Cloud Act, giving US authorities a right of access to data that is stored by US cloud service providers worldwide, is likely to add to the complex landscape.

On 16 July 2020, the EU Court of Justice, in the case known as *Schrems II* (C-3111/18), has declared the EU-US Privacy Shield as invalid and held that it does not include satisfactory limitations to ensure the protection of EU personal data from access and use by US public authorities on the basis of US domestic law. Owing to the ruling, cloud suppliers that have used the EU-US Privacy Shield as a basis for transferring personal data to the US must implement an alternative safeguard for the transfer to be lawful and renegotiations of cloud computing contracts is likely to follow.

Typical terms of service

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering material terms, such as commercial terms of service and acceptable use, and variation?

Commercial terms of service and acceptable use are commonly agreed on the basis of the supplier's standard cloud computing contract. Price model and payment terms vary depending on the services offered, however, services are commonly purchased as subscriptions and invoiced in advance. Provided that payment is overdue, the supplier may reserve the right to suspend the services immediately, however, sometimes excluding cases where payment is withheld in good faith. Principles for acceptable use commonly include customary restrictions, such as prohibition against redistribution of the services, use of the services for provision of outsourcing services and transmission of infringing material or malicious code.

As to variation, the supplier's standard cloud computing contract will, in many cases, include the unilateral right for the supplier to change the services, including the functionality and security. Such provisions may often be the subject of negotiations between the parties, for example, when the customer is a regulated entity and the provisions are in violation of the regulatory requirements applicable to the customer.

Typical terms covering data protection

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering data and confidentiality considerations?

In terms of data, cloud computing contracts have in recent years been greatly influenced by the statements and decisions of the Swedish DPA regarding the processing of personal data by cloud computing suppliers. These statements and decisions prescribe, among other things, that the customer must ensure that:

- a sufficient data processor agreement is entered into with the supplier;
- the supplier is not allowed to independently process personal data but only in accordance with the customer's instructions;
- the contract stipulates that Swedish law applies as regards the processing of personal data; and
- the customer is informed of all sub-processors involved in the processing of personal data type of services and the location of such sub-processors.

In addition, the customer should ensure that it is entitled to perform audits for the purpose of ascertaining the supplier's compliance with the customer's requirements on the processing and that a process for exit of the agreement is established, which safeguards that the supplier will not process the personal data post termination of the contract.

Moreover, the customer is, as a general rule, obligated to perform a legality assessment and risk and vulnerability analysis prior to entering into the cloud computing contract. The purpose of the legality assessment is to determine whether the supplier's processing of personal data under the cloud computing contract will be allowed under the data protection legislation. This includes measures such as ensuring that a data processor agreement is entered into, an assessment regarding cross-border transfers and any security measures necessary. The purpose of the risk and vulnerability analysis is to assess whether it is possible to assign the processing of personal data to the supplier and determine appropriate security levels and necessary measures that need to be taken in the light of the integrity risks involved.

Following the entering into force of the GDPR, it is currently not clear whether the above principles will be upheld by the Swedish DPA. As a minimum, the cloud computing contract normally includes provisions that comply with the requirements for a data processing agreement in the GDPR. Recently, some cloud computing suppliers have also started to provide details of the cloud computing supplier's processing of the customer's personal data in the capacity of data controller in the standard cloud computing contracts. Typically, such processing would be for the purpose of the cloud computing supplier's administration of the contract.

Confidentiality provisions are commonly mutual.

Typical terms covering liability

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering liability, warranties and provision of service?

Since the cloud computing contract in many cases is based on the supplier's standard contract, the supplier's warranties are normally limited. A typical warranty would imply that the services are materially consistent with the documentation, and that the supplier will not materially change the functionality of the services or the security of the services. Ultimately, the warranties may be subject to negotiation between the parties.

Limitation of liability is often mutual with a cap and excluding indirect and consequential damages. There is normally a carve-out for liability for death and personal injury and damages caused by intent or gross negligence. In some agreements, liability for breach of confidentiality is uncapped but with a carve-out for loss of customer data entered into the cloud services, which instead falls under the general liability in the agreement.

The supplier would normally provide indemnities for intellectual property rights (IPR) infringements caused by the proper use of the services and, correspondingly, the customer would provide for the IPR infringements caused by the proper use of customer data. You may also find other types of indemnities (eg, in case of violation of applicable law or customers' misuse of the services).

Service levels is a typical area where the cloud computing contracts are less flexible and the customer will in many cases have to accept the supplier's standard service-level agreements (SLAs). Penalties and similar possible remedies in the event of non-fulfilment of the SLAs are often limited to fairly low amounts and are sometimes a customer's sole remedy for such non-fulfilment.

Business continuity and disaster recovery plans could be necessary to implement as a result of the risk and vulnerability analysis performed by the customer prior to entering into the cloud computing contract and this would also normally be required by customers that are regulated entities.

Typical terms covering IP rights

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering intellectual property rights (IPR) ownership in content and the consequences of infringement of third-party rights?

The supplier generally reserves the IPR to the services and non-customer-specific content, whereas the customer reserves the IPR to customer data. Customary consequences of infringement of IPR normally apply (ie, modification of the services so that they are no longer infringing, obtaining a licence for the customer's continued use of the services or, ultimately, termination of subscription and refund of licence costs). The customer is often undertaking to indemnify the supplier for any claims made towards the supplier due to the content of the customer data entered into the services.

Typical terms covering termination

What are the typical terms of a B2B public cloud computing contract in your jurisdiction covering termination?

Either party will typically have the right to terminate the cloud computing contract in the case of material breach of the contract by the other party. Additionally, the customer often has the right to terminate the contract in cases where the supplier appoints a sub-processor that the customer on objective grounds refuses to accept. Following termination of the contract, the supplier will no longer have a right to process personal data for which the customer is the controller; however, the supplier is usually allowed a certain period of time to remove such data (up to 180 days are often seen, but it remains to be seen whether this period will change given the GDPR).

In some cases, the parties agree on a right for the customer to terminate the cloud computing contract prematurely (ie, termination without cause). The customer is then often obligated to pay an exit fee to the supplier corresponding to at least the supplier's anticipated revenues from the cloud computing contract.

The supplier may offer migration services on a time and material basis.

Employment law considerations

Identify any labour and employment law considerations that apply specifically to cloud computing in your jurisdiction.

The Acquired Rights Directive 2001/23/EC would (at least in principle) apply to a business customer entering into a cloud computing contract, provided that the cloud computing services are deemed to be outsourcing.

Law stated date

Correct on

Give the date on which the information above is accurate.

12 August 2020.

Advokatfirman Delphi - Dahae Roland and Peter Nordbeck