Six “Golden Rules” When Reviewing Cloud Contracts

Mark Adair and Philip Nolan

Mark Adair is a senior associate with Mason Hayes & Curran and advises both Irish and international clients on a range of complex technology matters. He has a particular focus in the areas of software, cloud computing, telecommunications and fintech. Mr. Adair is recognized as a thought leader in the Irish technology law sector and has authored a number of articles for Irish and UK technology publications and presented at national industry conferences.

Philip Nolan leads Mason Hayes & Curran’s Technology, Media and Communications team. His market leading international practice supports some of the world’s most successful tech companies in the fields of data protection, online sales, ad technology, international online law enforcement, IP licensing, cloud computing, social media law, and export control regulation.

More and more businesses are relying on cloud computing for their own use and to provide their services to end customers. Cloud computing, however, can be a complex and fast-moving technology and gives rise to a number of legal issues that parties need to address.

The following is a guide to help businesses and their counsel understand what boxes need to be ticked in the typical cloud computing contract. While most cloud customers will see data protection and cyber-security as obvious priorities, in this article we explore some of the other legal challenges businesses should consider when reviewing a cloud contract.

What Is Cloud Computing?

In broad terms, cloud computing delivers technology as a service on demand, over the Internet. In other words, a customer does not need to install stand-alone software or run its own applications and servers.

The cloud supplier hosts applications and provides the computing power to many different customers from the supplier’s data centers. This allows each customer to benefit from economies of scale and dramatically lowers the costs of obtaining a range of IT services.

Components of a Cloud Contract

Cloud suppliers usually include some or all of the following documents in their cloud computing contract bundle. These documents will need to be reviewed in conjunction with each other.

- **Terms of Service**: This sets out the general legal terms and conditions that govern the use of the service and the relationship between the supplier and the customer. Also known as the Terms of Use, it may incorporate other documents by reference.
- **Privacy Policy**: An extremely important document that sets out the cloud supplier’s approach to collecting, using, and protecting personal information.
- **Acceptable Usage Policy (AUP)**: Often used by social networks and cloud storage providers to specify permitted and prohibited practices when using the cloud service (e.g., prohibiting hate speech or forbidding use of the service to deliver spam).
- **Service Level Agreement (SLA)**: The SLA documents any target levels of service availability and other metrics and, possibly, service-level rebates that the cloud supplier offers.

When reviewing the various documents that make up a cloud contract, a business should consider the impact of the following six golden rules and if necessary seek legal advice on them.

1. **Liability**

When reviewing a cloud contract, customers and their legal advisers should consider carefully the issue of liability.

Cloud suppliers often will attempt to provide the services “as is” with no warranties regarding service availability or quality. It is common for suppliers to exclude liability in the event of loss of data or a service...
outage, along with other forms of direct and indirect loss.

As cloud services are becoming increasingly common, however, customers are putting more data onto the cloud and their own end-users also may be relying on the cloud service. In light of this, the consequences of unavailability or loss or corruption of data could be substantial.

A customer should consider whether it requires the cloud supplier’s liability to be unlimited in certain scenarios, such as the supplier’s breach of the data protection, privacy or confidentiality provisions of the contract.

2. Intellectual Property Rights

A typical cloud contract may state that use of applications only provides the customer with exclusive use of the cloud service rather than outright ownership in the intellectual property rights (IPR) created through it. The customer should consider whether it or the cloud supplier should own developed material and use-specific adaptations. The IPR clause in the contract should reflect the agreed positions.

3. Hidden Charges

There generally are two types of cloud models that a supplier will offer: (1) premium paid services and (2) free services.

Cloud suppliers usually provide paid cloud services on a utility basis under recurring billing, for example, monthly. The supplier usually calculates the customer’s charges based on either the number of users or the particular service options that the customer selects.

Alternatively, under a free cloud model, the customer does not pay any upfront or recurring fee but the cloud supplier may generate revenue by using the customer’s personal data to provide targeted advertising within the service.

With either model, customers need to review carefully the cloud contract for any hidden charges, in particular charges incurred when the user exceeds thresholds for storage, set-up fees, security and back-up, support and maintenance, upgrades and premium fees.

4. Termination of the Contract

Depending on the type of cloud service, a supplier may impose a minimum service period in the contract. Customers should be aware of the possibility of early termination charges if a fixed-term cloud contract is concluded earlier than expected.

Equally, customers should err on the side of caution in relation to the notice period in the contract for nonrenewal or cancellation. If the cloud supplier only has to provide one month’s notice of non-renewal or cancellation this could leave the customer stranded with insufficient time to engage an alternative supplier.

5. Governing Law and Jurisdiction

A cloud customer should check the governing law and jurisdiction clauses to determine where it is able to enforce the terms of the contract, if an issue arises in the future.

Some standard-form cloud contracts also enforce arbitration on the parties, which may limit the ability of certain customers to make a claim in their local courts.

6. Lock-in and Exit

Customers should be cautious in relation to over-dependence on one cloud supplier.

A customer ideally should include a provision in the contract allowing it a grace period after termination or expiry of the contract to recover its data and an obligation on the supplier to make sure user data is adequately deleted afterward.

It also is useful for the contract to contain a provision stating what transition-out assistance the cloud supplier has to provide and whether this will come at an additional cost.

Importance of Planning Ahead

When a customer is choosing a cloud supplier one of the most important things is to plan ahead and review the contractual and pricing documentation well in advance. While many cloud suppliers offer free services, this may not always be the best option for the customer in the long run.

When selecting a cloud supplier, a business should consider not only the upfront or monthly service fees but also whether the proposed cloud contract has suitable protections in place. To maximize the benefit the customer will receive from the cloud service, it should ensure that the cloud contract suitably addresses the “golden rules” of liability, intellectual property, hidden charges, termination costs, governing law, and transition-out requirements.