Negotiating Contracts: 12 Key Terms to Negotiate in a Software as a Service or Cloud Service Agreement

By Stephen F. Pinson
Scott & Scott LLP



Image by Yoel Ben-Avraham

Software as a Service and Cloud Service offerings have become ubiquitous digital platforms for many enterprises and small businesses in their quests to provide a single unified platform to their employees and customers. Providers offering Software as a Service and Cloud Services allow end users to access software and infrastructure remotely from any location and storing data with a provider. Because of the risks associated with storing data in the cloud and the need for uninterrupted access to the data, businesses want to be sure that they understand their requirements when entering into a cloud service agreement with a provider. The following is a list of suggested requirements when negotiating Software as a Service or Cloud Service agreement (these are not in any particular order):

1. Demarcation

A demarcation point is typically defined to establish the point at which the service provider's obligations under the contract end and the customer's responsibilities begin. Demarcation points are often used in warranties and service level agreements to assure customers that services will be

provided up to the point of demarcation. This creates a clear delineation of responsibility to calculate service level credits, and anything that occurred on the customer's side of the demarcation point, will not be a breach of warranty or entitle the customer to service level credits.

2. Service availability

Service availability relates to the ability of a business to access the software and/or the data at all times. Businesses want to ensure that they have access to the provider's services and the ability to retrieve and use the data stored on the provider's systems. Service interruptions generally occur when: a server is down, the internet connection fails, provider withholding service because of a fee dispute, natural disaster at the data center, or the provider closing its doors because of bankruptcy. In any event, business should insist that provisions covering service availability and service levels are outlined in the agreement.

3. Service levels & Service Level Credits

There are two general approaches to service levels or service guarantees. One is the time it will take the service provider to respond to an incident, the other is the guaranteed availability of the systems (i.e., uptime). Service levels are typically outlined in a service level agreement (an SLA). The contract should outline what the provider will guarantee in terms of uptime or response times. If the provider fails to meet the guarantees, the contract should outline whether the end user can request a service level credit. Additionally, business should consider including a right to terminate if the provider consistently fails to meet the service guarantees.

4. Data – Ownership rights, security, backups, and conversion

Business customers must be mindful that their data is among the most important information they own, and ensuring the cloud service provider treats that data appropriately should

be one of the paramount issues when negotiating a cloud service agreement. Business must ensure that they own the data, understand how the service provider can use, aggregate, or manipulate the data, and identify its requirements for the provider to protect the security and confidentiality of the data. The business should make sure that the cloud service provider agrees to a specific schedule for performing and testing backups.

5. Insurance

Good cloud contracts should always address what insurance the parties must carry. Cloud service providers should maintain insurance for instances of data loss that cause business interruptions. End users should consider first-party insurance that will cover expenses related to data loss or breach.

6. Indemnification

Indemnification requires one party to pay for defense costs and any damages awarded when a third party makes a claim against the other party. It is critical for the parties to understand when they will be required to indemnify the other party and whether the limitations of liability will apply to an indemnification claim. It is important to ensure the contract provides indemnification for data and security breaches as well as intellectual property infringement.

7. Limitation of liability

One of the most important provisions in a cloud or software agreement is the limitation of liability that applies to either party in the event of a claim or dispute between the parties. A good limitation of liability provision will balance between the potential financial losses the customer can incur and the financial risk the provider is willing to take given the revenue the project will generate. In many instances, the parties will negotiate a relatively low limitation of liability, e.g., one year of services and then carve out some

claims that are less likely but can be significantly more costly. These carve-outs include: indemnification obligations, confidentiality obligations, claims covered by insurance, and infringement claims (this is not an exclusive list).

8. Warranties

Generally, cloud service contracts contain many of the following warranties: (1) that the service will materially conform to the documentation, (2) the services will be performed in a workmanlike and professional manner, (3) the provider will provide the necessary training for the customer to use the services, (4) the services will comply with federal and state law(s), (5) the provider has sufficient authority to enter into this agreement, and (6) the parties have the authority to enter into the agreement.

9. Intellectual property

The parties can often overlook intellectual property rights when negotiating a cloud service agreement, but this oversight can be costly. In instances where the provider will develop products or implement services, the parties should clearly identify who will own any intellectual property that results from the development or implementation.

10. Implementation

When the provider will perform implementation services, the parties may choose to identify those services in a Statement of Services or Statement of Work. A good statement of work will include all the services that the provider will perform and should also include any services that will be excluded.

11. Term, Termination, & Transition Services

The term of a cloud service agreement varies but can be based on a yearly subscription. Some agreements have automatic renewal provisions. Parties should clearly identify when and

if the parties can terminate for convenience, whether there are cancellation penalties, whether the provider can increase service fees on a periodic basis, and whether the provider will transfer the business' data at the end of the relationship. If there is a transfer provision, the parties should also specify the acceptable formats for data delivery.

12. Fees

When the provider calculates service fees based on the number of users or devices, the end user should have the ability to adjust the users on a periodic basis to reflect the actual number of users or devices.

Conclusion

Whether you are a service provider or an end user, cloud agreements can help you understand your rights and your obligations. While there are many new issues when a third-party is holding sensitive data in its environment, a good services agreement can minimize misunderstandings and protect each party.