Cloud Service Contracts: Breaking Down the All Important Service Level Agreement (SLA)

By: Kaiser Wahab and Lauren Mack

For many businesses, storing company and customer information in the cloud may seem like the cheapest and most convenient option. Too often however, businesses rarely realize that with one-click ease they are putting critical data (personal info, trade secrets, intellectual property, etc.) in the crosshairs of a security disaster, due to compliance issues over privacy, data security, and other laws and regulations. Hence, the ease of a cloud solution can lead to a legal headache if a strong contractual foundation is not put into place. The most critical of those contracts may be the **SERVICE LEVEL AGREEMENT** ("SLA") between the client and the cloud service.

By making both parties aware of their responsibilities and when they may be held liable for failing to live up to those responsibilities, a strong SLA can help prevent many of the hassles and dangers that can come with switching over to the cloud. This article provides insight into the major parameters and provisions that drive the SLA.

The provisions of an SLA generally fall into ***three broad categories***:

1. Data Processing and Storage;
2. Infrastructure and Security; and
3. The Provider-Client Relationship.

1. DATA PROCESSING AND STORAGE

Ownership of Data – For any business, it is imperative that the SLA clearly state that the client retains all ownership in the data it stores with the provider. This is especially important if the business plans to store any copyrighted, trademarked, or patented content or other proprietary data to which it owns the rights. Depending on the nature of the services, businesses may also want to clarify the ownership of the product of any data processing that occurs on the provider's system.

Access to and Use of Data – The agreement should stipulate that the client has the right to access and retrieve any of its data stored by the provider. For situations in which there is an emergency and data needs to be accessed right away, a procedure and timeline should be in place for the client to quickly address time-sensitive matters. Businesses may also want to consider a provision prohibiting the provider from using the data for any purpose other than the agreed upon services or from allowing third parties to access and use the stored data.

Location of Data – Because the stored data's physical location determines many of the laws that will apply to it, it is very important for the client to know in what jurisdiction its data will be located. The laws of that jurisdiction will govern who can access the data, how it must be stored, and how security breaches must be handled. It is often the client's responsibility to make sure that it complies with these laws, but it cannot know what laws it must obey without knowing where the data resides. The provider may need to certify that it complies with the European Union Data Protection Directive if personal information about citizens of EU countries will be stored in its infrastructure. Businesses must be aware of and make sure that the provider complies with any other foreign laws governing the storage or transfer of the personal information of that country's citizens that may apply. Clients should also be cautious of violating United States export control regulations if certain types of data are "exported" to a server outside of the United States.

Government Requests for Access to Data – The SLA should also address what will happen if there is a subpoena or other government request for the client's data. It should contemplate whether the client will be notified before or after the provider discloses the data (if the client is notified at all) and what the provider's obligations are if the client decides to contest the order. Clients may also want to include a provision requiring the provider to limit the disclosure of the business' data as much as possible when responding to a government order.

Data Retention and Deletion – State, federal, and international laws may govern the retention and deletion of the client's data. If the business has a data retention policy, the SLA should bind the provider to those same procedures to ensure that retention requirements for certain types of data are complied with and, in the case of a lawsuit, any discovery obligations.

Metrics – The SLA might also describe several technical aspects of the provider's service so that the client knows what kind of performance it should expect, including how quickly it responds, how often it is available, how likely the data is to be lost, the maximum amount of storage or bandwidth, how well the system performs as load increases, the percentage of requests that are handled automatically, and how quickly the provider responds to a service request. A penalty for failing to meet these standards may be built into the contract, as well as incentives for meeting or exceeding them.

2. INFRASTRUCTURE AND SECURITY

Data Security – Depending on the type of data and the location where it will be stored, the SLA may need to require a specific minimum level of security to comply with state, federal, and foreign laws. Clients should know what level of security their data must have to comply with any applicable laws and make sure that the SLA holds the provider to those minimum requirements or higher.

Security Breaches – It is very important that a SLA define what constitutes a security breach. This could range from a narrow definition, such as a breach of the security obligations set forth in the agreement, to a broader definition, such as "any actual or reasonably suspected unauthorized use of or access to provider systems or unauthorized disclosure or alteration of client information." Although some state and federal laws already require providers to notify clients of a security breach, breach notification procedures should be in place to govern how and when the client will be notified, as well as any other details concerning the breach that need to be communicated to the client. The SLA may require the provider to investigate the breach, use its best efforts to mitigate the breach's impact, collect evidence surrounding the breach, and document its response. If the breach is due to an error on the part of the provider, the agreement may make any resulting damages or fines the provider's responsibility.

Disaster Recovery – The client should be aware of how much redundancy there is in the provider's system to ascertain its ability to prevent outages and how the provider plans to continue to supply uninterrupted service if there is a disaster or other unforeseen event. There should be notification procedures for when the service is down or data is damaged, and the agreement should also specify under what circumstances the provider must compensate the client for service outages or damaged data.

Maintenance – Clients may want to contract for advance warning when maintenance tasks will be performed on the provider's infrastructure and whether the service will be down or slowed during that time.

Right to Audit – The client will often want an annual right to audit the provider's security to make sure that it is complying with all security requirements in the agreement, as well as any applicable privacy and data security laws. An audit right is also useful in determining any system vulnerabilities, whether data transfer restrictions are being complied with, whether the data retention policy is being followed, and whether the data is properly deleted after termination of the relationship. How and when the audits will occur should be determined, as well as any fees or limits the provider places on the audit, such as a cap on provider labor costs incurred as a result of the audit.

3. PROVIDER-CLIENT RELATIONSHIP

Price Caps – The Client may want to contractually limit the amount that the provider can increase its fees each year by creating a price cap based on a percentage increase or what the provider charges its other customers. Clients who plan ahead will also want to negotiate the costs of any expansions of volume or usage in the future.

Functionality – Since cloud computing is constantly evolving, providers often update their infrastructure, including adding and deleting features. Clients may want to ask for notification whenever the provider plans to delete functions or features enough time in advance for the Client to be able to switch to another provider if the update creates problems for the business.

Vendor Outsourcing – When a cloud user contracts with a provider, it is not always necessarily the case that same provider hosts the cloud user's data. That provider may contract with another provider for cloud services, who may then turn around and contract for cloud services from yet another provider, to the point where neither the Client nor the original provider know where the Client's information is actually being stored. As discussed above, there are several reasons why the Client must know the location of its data. The SLA should address whether the provider may outsource its services, whether the Client must be given notice and approve of any subcontractors, and whether the subcontractors must also comply with the SLA or meet other security standards.

Limitations on Liability – Both parties should be aware of how much liability the SLA allocates to the provider. Some agreements may narrow the scope of information or the circumstances under which the provider is liable in the event of a breach or cap the amount of damages it will be responsible for if it is liable, while others will leave the amount of the provider's liability in the event of a security breach unlimited.

Indemnification – Many provider contracts do not include an indemnification provision, but a clause indemnifying the Client for any security breach or breach of applicable privacy laws caused by the provider can save the Client a lot of time, money, and hassle. The indemnification clause may include expenses beyond those associated with claims, litigation, and fines to cover the cost of notifying customers, employees, and regulatory bodies; investigating, assessing, and remedying the breach, including by providing crediting monitoring or other services to those affected by the breach; hiring public relations consultants; and responding to government investigations.

Termination – Who may terminate the contract as well as when and why must be included, along with any associated fees or refunds. The SLA should also describe how, when, and in what format the data will be returned to or retrieved by the Client upon termination. If the provider stores data in a format that is not accessible by the Client, this could become a problem when the Client attempts to switch providers if the format is not specified. Once the data has been successfully transferred to the Client, the contract should require the provider to destroy its copies of the data.

Conclusion – While there is no template SLA and each cloud solution vendor is unique, the above is a good roadmap to understanding the general issues. Moreover, with that insight, better terms can be negotiated to address your operation's unique concerns. Certainly, if a vendor's SLA is light on details that alone may be an indicator that the vendor is light on accountability.

ATTORNEY ADVERTISING. Results depend on a number of factors unique to each matter. Prior results do not guarantee a similar outcome.