KILPATRICK TOWNSEND

10 KEY TAKEAWAYS

The Impact of Adopting New Technologies on the Negotiation of Cloud-Based Contracts

Kilpatrick Townsend's Farah Cook recently participated on a panel discussion, "The Impact of Adopting New Technologies on the Negotiation of Cloud-Based Contracts," at the 36th Annual National Bar Association Commercial Law Section Corporate Counsel Conference. The session outlined the areas of tension that arise when negotiating Software as a Service (SaaS) contracts that involve cloud-based and other innovative technologies, including Software License Agreement considerations, and recommended best practices for both technology SaaS and SLA transactions.

Ms. Cook's 10 key takeaways from the discussion include:

1

Every day, innovative technologies are changing the way companies do business. Legal advisors must understand the added features and complexity, contained in new technologies, which create additional vulnerabilities. Since adaptation of technology is key to business survival, purposeful conversations about technology strategy must continue so as to understand how business strategy aligns with the risk of adoption.

Always remember the basics. Regardless of the new technology, whether the transaction involves on-premise software or is cloud based, indemnities, intellectual property ownership, limitations of liability, and warranties are still important. At the core of all contracting, certain key considerations remain. Service levels, data security, indemnities, and limitations of liability continue to be some of the most hotly negotiated provisions, and a company's approach to these items should always reflect its overall risk tolerance irrespective of the specific technology at hand.

2

3

Generally, cloud services agreements have a shared basic structure with key terms and provisions in common. However, each individual SaaS, PaaS, or IaaS agreement will have unique requirements that depend on the product, services, and industry. SaaS Agreements are focused on the software and data that are hosted by the Vendor and accessed by the Customer over the internet. PaaS Agreements enable the Customer to create its own SaaS applications that are then hosted, so the agreement is more technical to cover development, testing, and deployment environments. IaaS Agreements must also cover the physical equipment that a Customer outsources to the Vendor, which makes it more of an outsourcing arrangement.

Service Levels are still important in innovative technologies. Vendors and Customers will differ on approaches to negotiating service-level credits, and the Customer's ability to negotiate will often depend on whether the solution is hosted on a public, private, or hybrid cloud. Common landing spots include compromising on increased credit amounts and setting higher standards for Vendors through service-level termination events. Use an online uptime or availability calculator to understand what the percentage of availability truly means, and always study the definitions and evaluate the formulas for intended consequences.

4

As technology changes and emerges, warranties are still critical and the list of warranties may increase. Over the last few years, the inclusion of a "no malicious or disabling code" as a warranty has become increasingly important as have the definitions of "disabling and malicious code". Threat actors evolve as quickly as technology

5

disabling code" as a warranty has become increasingly important as have the definitions of "disabling and malicious code". Threat actors evolve as quickly as technology, thus the methods of introducing these codes and the types of code require lawyers to continually expand the definitions of "malicious and disabling code". In addition, the inclusion of compliance with laws and third-party consents warranties are commonplace for cloud agreements.

Indemnification provisions are still one of the most negotiated provisions in cloud transactions. Customers will, of course, negotiate the broadest indemnity possible to cover all damages, losses, and liabilities for a series of events, such as confidentiality, security, intellectual property infringement, gross negligence and, in some circumstances, personal injury and property damage. Vendors are trending towards a limited defend and pay indemnity to ensure that the Vendor is only responsible for amounts finally awarded by a court based upon a narrow list of occurrences, such as non-infringement with exclusions. From the Customer's perspective, it is important to remember that breaches of confidentiality and security, data privacy violations, and IP infringement may not be sufficient to cover all damages associated with those claims. However, despite the trend, a common landing spot is still a third-party claims trigger with negotiated indemnifiable events. For emerging technology solutions, one of the most important practice pointers is to remember that certain exclusions to the IP infringement indemnity could undo protection (such as integration with third-party systems).

6

7

There is no market standard limitation of liability provision. The one exception to this statement is that super caps are the trend for certain breaches, such as data security; however, they vary drastically in amounts (i.e., a set amount, or 2x or 3x the general cap, or even more). A few practice pointers include asking whether carve-outs apply to both the damages cap and the consequential waiver; what are the "direct damages" (i.e. consider including a definition for acknowledged direct damages); and is it clear that amounts paid under a carve-out or super-cap do not erode the general damages cap?

Maintaining control over privacy and customer data is still a vital part of effectively managing risk. Generally, the party "owning" the data has the ability to exercise control over who can access or use the data and dictate that its privacy policy applies. Ownership in data is often noncontroversial, and Vendors readily accept Customers owning all "customer data" or "inputs" uploaded into the cloud service. However, gaps may remain compared to ownership of "outputs" generated by the cloud service, hinging on the definition of "customer data" in the cloud agreement. From the Customer's perspective, a narrow definition of customer data may not capture other data beyond "inputs" derived from the Customer's use of the cloud service that may have customer-specific or sensitive information that the Customer wants to control. A cloud provider, however, may find it operationally challenging to agree to a broad definition of Customer data, as it may prevent the cloud provider from using certain data or insights to improve its solution or provider services to other Customers. The cloud provider also may not be practically capable of applying more stringent data science limitations to a single Customer's data (or a provider may claim such impracticability during initial negotiations).

8

9

Scrutinize aggregated data provisions. As the cloud market matures and providers seek competitive advantage, providers increasingly insist on unfettered rights to collect and use broadly defined "aggregated data", not only for internal business purposes but also to monetize such data with third parties. While such broad usage rights may be coupled with enticing pricing and product enhancements, the permitted scope of usage and aggregated data must be closely scrutinized, particularly if sensitive, regulated or customer-specific data is involved that may not be effectively aggregated and anonymized in a manner that continues to maintain customer confidentiality or compliance with applicable laws. Such use, for example, may undermine a provider's "processor" or "service provider" role on which a customer relies for data protection law compliance. Additionally, the Customer should negotiate a suitable customer liability disclaimer and indemnity for a provider's use of aggregated data.

Through a risk-based vendor management system, the incremental risk of relationships with third-party Vendors can be tailored to align with business goals. As part of protecting assets, minimizing liability, and safeguarding reputations

relationships with third-party Vendors can be tailored to align with business goals. As part of protecting assets, minimizing liability, and safeguarding reputations, organizations must examine Vendors carefully to assess if a selected Vendor is the right fit. With an increasing number of Vendors entering the market, understanding a Vendor's financial strength, customer base, security protocols, and operations may help Customers avoid Vendors that do not align with their long-term strategy and goals.

10

For more information, please contact Farah Cook: fcook@kilpatricktownsend.com

www.kilpatricktownsend.com