KILPATRICK TOWNSEND

10 KEY TAKEAWAYS

Top 10 Takeaways for In-House Counsel When Negotiating Data-Related Issues in SaaS, PaaS and IaaS Cloud Contracts

By Sonia Baldia (Partner) and Jeff Connell (Associate), Technology Transactions, Kilpatrick Townsend LLP

Kilpatrick Townsend attorneys Sonia Baldia and Jeff Connell recently presented at the "Association of Corporate Counsel Dallas-Fort Worth: 2023 Annual In-House Symposium" in Frisco, Texas. As businesses continue to accelerate cloud adoption and digital transformation efforts, in-house legal counsel must protect one of their company's most valuable assets: data. Data is an increasingly complex topic that permeates throughout various provisions of a potential cloud transaction, and navigating the contractual controls is largely dependent on the applicable cloud solution or technology at hand, whether SaaS, IaaS, or PaaS. Their session offered practical guidance on how to effectively navigate the risks inherent to data and provide strategies to negotiate cloud agreements that better address and protect valuable data.

1

Data vulnerability remains top impediment as businesses embrace the cloud. In cloud contracts, a top concern for in-house counsel is to mitigate risk to the company data migrated to the cloud, which is frequently amongst the company's most valuable or critical assets. A host of critical issues arise when data rears its head in SaaS, PaaS, or IaaS contracts. Is the data secure in the cloud service? Who can access and use it? Where will it be hosted? Will it be transferred to or accessed from offshore locations? Is the cloud service compliant with the applicable regulatory requirements? Will the provider implement requisite operational and technical measures to safeguard data? Which party is liable for data breach? Is the provider carrying sufficient cyber liability insurance to cover liability risk? Unlike traditional on-premise computing, where a customer has greater control over its data, cloud services often require a customer to relinquish control over its data to the cloud provider. This significantly amplifies a customer's concerns over data access, security and liability, and a provider's competing concerns over potentially excessive customer restrictions, intrusive audits, and overexposure to liability for data breach. Customers and cloud providers alike must navigate the risks inherent to data and negotiate cloud contracts that attempt to balance each party's risk and liability relative to data.

2

Determine data "risk profile" to tailor contractual controls. Not all data is the same, and no one size fits all when negotiating data-related provisions in cloud contracts. The type of data involved and the type of cloud service at hand typically drive the scope of provider diligence and data protections sought in the cloud contract. To determine data's risk profile, a customer needs to know upfront what data is flowing to the cloud, what is happening to that data in the cloud, what data is flowing back to the customer, and what data may be flowing to third parties.

Contractual controls can then be tailored to fit the data risk profile. For instance, the risk rating is high if personal data (e.g., PII or PHI) or consumer data will be processed in the cloud service. In this instance, parties typically negotiate a robust data processing agreement (DPA) to regulate collection, access, use, disclosure, storage, transfer and return of such data in compliance with applicable laws, including data privacy laws. In-house counsel should watch out for service provider DPAs that attempt to separate the DPA liability from the master contract or carve out certain data from the DPA's scope.

3

Evaluate vendor risk with internal stakeholder engagement. Each cloud provider presents varying risk relative to customer data and therefore is subject to varying standards of security performance commensurate with data criticality, service category and compliance needs. In IaaS and PaaS, a customer is responsible for managing and securing the applications and data layers of the cloud stack, unlike in SaaS where a provider is responsible for securing all layers of the cloud stack. As such, each party's security responsibility will vary depending on the cloud service. Service provider documentation frequently attempts to shift data risk and liability to customers. In-house counsel must engage with internal stakeholders and subject matter experts early on in the vendor selection process to assess vendor risk and design the cloud solution and contractual protections accordingly to safeguard customer data and appropriately allocate liability.

4

Owning data empowers greater control on data. 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 frequently non-controversial, and vendors readily accept customers owning all "customer data" or "inputs" uploaded onto the cloud service. However, gaps may remain relative to ownership of "outputs" generated by the cloud service, hinging on the definition of "customer data" in the cloud contract. From a customer's perspective, a narrow definition of customer data may not capture other data beyond "inputs" derived from customer's use of the cloud service that may contain customer-specific or sensitive information that a 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 preclude the provider from using certain data or insights to improve its solution or provide services to other customers. The 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).

5

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 undo a provider's "processor" or "service provider" role on which a customer relies for data protection law compliance. Additionally, a customer should negotiate an appropriate customer liability disclaimer and indemnity for a provider's use of aggregated data.

6

Who's data security and privacy policies govern – customer's or provider's? The answer is generally more nuanced than a customer simply insisting that its own security policies govern the cloud service. Typically, a SaaS, PaaS or IaaS provider cannot customize the security and privacy configurations of its solution for each customer given a shared resources model, and customizations may add significant cost to customer. In-house counsel should work with their information security team to conduct a gap analysis between the customer's security requirements and the provider's security policies (including configurations and an incident response plan) and address material gaps in the cloud contract through additional protections, such as data segregation, localization, encryption, masking, penetration testing, background checks, certifications, and annual SOC audit reports.

7

Hold the cloud provider responsible and liable for its cloud vendors. Many cloud providers rely on other cloud vendors to support their cloud offerings. For instance, a SaaS provider may host its solution with a cloud platform or infrastructure provider. Cloud providers often resist a customer's prior approval rights with respect to their cloud vendors and seek to disclaim liability for such third parties. Such a liability disclaimer can significantly undermine a customer's ability to enforce its rights and remedies against the cloud provider or its third party if such third party were to violate any terms of the cloud contract or otherwise misappropriate customer data in its control due to the lack of privity of contract between the customer and the provider's third party. The customer should not only unequivocally hold the cloud provider responsible and liable for the acts and omissions of its cloud vendors but also consider if other contractual terms, such as insurance, audits, and termination rights, should flow down to such third parties.

8

Location, location, location. It may sound counter-intuitive to the ubiquitous cloud model, but data location matters as it may inadvertently trigger not only operational vulnerabilities but also regulatory compliances, data transfer restrictions and compelled disclosure relative to customer data in home and host jurisdictions (e.g., export control, OFAC, GDPR, GLBA etc.). This can be particularly problematic if regulated data or business sensitive data is involved. Typically, cloud agreements do not offer visibility into provider's data transmit or storage locations or from where a provider's affiliates or subcontractors may access the data, but customers must demand such visibility if regulated data or sensitive workloads will be migrated to the cloud to be able to determine any necessary geolocation requirements on data flow. Complex rules on data sovereignty, data residency and data localization are rapidly emerging across jurisdictions that directly impact the level of control a jurisdiction may exercise over the data and subject stakeholders to substantial liability for non-compliances. The location risk should be addressed in the cloud contract by clearly stipulating the applicable geographical restrictions relative to the data and subjecting any changes to location during the contract term to robust change control process.

9

Data breach liability remains heavily negotiated in cloud contracts. Each cloud provider has a different threshold, and each customer has different leverage, in negotiating indemnity and liability clauses relating to data. Customers expect cloud providers to accept liability for data breach caused by their failure to comply with contractual security obligations, whereas providers attempt to shift liability to customers or at least drastically narrow the circumstances in which they may be held liable. For example, a provider may negotiate super caps to limit their liability. In-house counsel should pay particular attention to excluding consequential damages in the cloud contract because certain U.S. courts have held data breach losses to be consequential. Therefore, a customer may consider defining the anticipated data breach damages (such as credit monitoring, investigation and remediation) as direct damages in the contract to avoid uncertainty regarding its ability to recover such damages under the contract. The key to negotiating successful cloud contracts with appropriate allocation of liability for data breach amongst the parties, commensurate with the deal value and transaction risk, is to understand the nature and scope of data and the cloud service involved and its interplay with the data-related terms in cloud contracts. To understand risk, in house counsel should consider, among other factors, if a breach would expose a customer's "crown jewel" trade secrets, erode user trust, or trigger consumer class actions.

10

Cloud vendor bankruptcy is a rising concern in current economic environment. A cloud vendor's bankruptcy can be a customer's worst nightmare because not only can it potentially disrupt the customer's use of the cloud service but it can also severely curtail customer's ability to retrieve its own data stored in the cloud service. Typically, upon initiating a bankruptcy proceeding, an automatic stay is imposed which prohibits all adverse actions against the debtor in an effort to preserve the bankruptcy estate for the benefit of the creditors. If a cloud vendor initiates bankruptcy proceeding, not only may the customer be prevented from terminating the cloud contract but worse yet the data may be considered the property of the debtor's estate and may be monetized to pay off the cloud vendor's creditors, thereby potentially creating significant liability for the customer. Accordingly, it is imperative for a customer to keep a finger on its mission critical cloud vendor's financial pulse for early warning signs to appropriately manage this risk. The customer must also build into the cloud contract certain pre-bankruptcy and bankruptcy-proof rights and remedies to facilitate prompt data recovery and limit customer's exposure in the event of vendor's bankruptcy.

For more information, please contact:
Sonia Baldia, sbaldia@kilpatricktownsend.com
Jeff Connell, jeff.connell@kilpatricktownsend.com