Matthew Cavarra

Partner
303.295.8169
Denver
mncavarra@hollandhart.com

Considerations for Customers When Contemplating SaaS and Hosted Technology Solutions

Considerations for Customers When Contemplating SaaS and Hosted Technology Solutions

Insight — February 27, 2017

Negotiating legal terms with SaaS and hosted technology providers are constrained by the provider's offering and the terms and conditions previously adopted by other customers of the provider; nonetheless, these terms and conditions are often negotiable. Customers should consider proposing appropriate revisions based upon (1) the criticality of the services to the customer, (2) the sensitivity of the data the provider will host, and (3) the size of the transaction.

Many of the following issues can and should be subject to diligence in advance of negotiating the agreement, with the agreement being a vehicle to obtain ongoing commitments throughout the lifecycle of the customer's relationship with the provider. During such efforts and discussions, the customer may discover that the provider has a solution more appropriately tailored to the customer's needs, or identify that the least expensive solution is not necessarily the best fit. While not an exhaustive list, customers should, at a minimum, think through the following considerations when selecting and negotiating with SaaS and hosted technology provider(s):

- **Service Levels (SLAs)**
  Consider not only the “uptime” SLA of the provider's system, but also appropriate SLAs for support response and resolution times as well as latency concerns, all of which may impact the value of the provider's offering. Determine scheduled downtimes, and confirm these align with anticipated hours of reduced activity on the system. Understand how the provider measures and reports the SLAs, and what remedies are available if SLAs are missed.

- **Disaster Recovery/Business Continuity**
  What measures are put in place by the provider to mitigate against the risk of the system going down? Customers should obtain and understand the provider's disaster recovery plan and policy and find out how often such plan is tested. If the system is “mission critical,” confirm system redundancies (including appropriate geographical diversity) and determine whether a “hot” or “warm” redundant system is required and/or available.

- **Data Security**
  Identify what type of data will be hosted by the provider, and

compare the provider's security policies against the customer's policies. Obtain information regarding the security audits that the provider has performed and determine what audits will be performed going forward. Determine where the data will be stored, the implications of cross-border usage, and the security protocols of the provider's data centers.

- **Privacy**
  Will the data hosted by the provider relate to “kids, cash, kidneys, or contacts” (i.e., minors, payment card or financial accounts, healthcare, or personal information)? This type of data is subject to heightened regulatory schemes, both in the U.S. and abroad. Further, obtain an understanding from the vendor how it complies with applicable laws, and what commitments it will undertake for the provider's violations of such laws and/or for causing the customer to violate its duties under applicable laws. Understand which privacy policy(ies) will govern the usage of the system, and be sure commitments remain.

- **Data Retention and Usage**
  With which entities will the data on the system be shared? How will the provider use the data from the customer and its authorized users? How long does it store the data and what methods are used to destroy the data? What happens if the customer's data is subject to a “legal hold?” Confirm the provider's responses against the customer's policies, including its data retention and privacy policies.

- **Onboarding/Data Conversion/Transition Assistance**
  What commitments does the provider make to help get to “go live” onto the provider's system? Of equal or greater importance, what commitments will the provider make to transition away from the system at the end of the agreement? Consider speaking with the provider's past and present customers about their migration experiences.

- **License Grant**
  Be sure the license grant corresponds both to the expectations of the commercial terms, but also to assure that it is broad enough to permit the customer and its intended users to undertake all activity and use all functionality it reasonably anticipates will be necessary to utilize, and migrate to and from, the solution.

- **End User License Agreements**
  Determine whether users will need to consent to or accept any additional terms and conditions relating to the solution. Verify that any such terms are acceptable and do not expose the customer to unanticipated liability, nor conflict with the terms and conditions mutually-agreed upon as part of the negotiation process.

- **Warranties/Indemnities/Risk Allocation/Liability Limits**

To what extent, if at all, is the provider warranting its system and the services? Many providers include appropriate covenants, representations and warranties, but then limit the extent the provider “stands behind” these commitments by capping the liability. Determine the liability caps and consider standard carve-outs, including violations of law, security breaches, breaches of confidentiality, infringement, and indemnifications. Protect against third party claims by inserting appropriate indemnity and defense provisions, including for violations of privacy laws and intellectual property infringement.

- **Insurance**
  Evaluate the provider's insurance coverages and confirm the provider will commit to carry appropriate coverages during the term of the agreement, for so long as the provider hosts customer data and a reasonable period beyond for which the customer may still have rights to bring covered claims. In particular, analyze the provider's cyber security coverages to determine what security and privacy breaches are covered, and which exclusions apply.

- **Force Majeure**
  A “standard” force majeure provision is not appropriate for these types of agreements. Specifically, the provider's systems and services should be designed and operated to reasonably anticipate criminal conduct (e.g., hack attempts, terrorist activity) and weather events (e.g., fires, floods, earthquakes) that under other circumstances might be considered “beyond the provider's reasonable control.”

Third party hosted solutions often save customers time and money, but – as with any procurement decision – each requires forethought and a careful understanding of the responsibilities and risks associated with the transaction. Taking proper steps to understand and mitigate legal risks helps maximize the benefits that leveraging hosted technology may offer.
