CONTRACTPROBE

Key Clauses to Include in Software as a Service Agreements

Software as a Service (SaaS) agreements present unique legal challenges for businesses. They combine the typical sticking points of ordinary supply agreements with the specialised areas of data security, privacy and intellectual property rights. In addition SaaS supply agreements are nearly always drafted by the supplier and are often presented on a "take it or leave it" basis.
The following are some key issues for customers to consider when reviewing SaaS agreements. If the draft agreement is unsatisfactory on a key matter, and the supplier is not willing to change its terms to address the customer's concerns, then the customer might have to consider engaging another supplier or take its own mitigating steps to manage the relevant risk.

1. Scope of Services

Customers should ensure that there is a clause clearly setting out their permitted use of the software product in the cloud. This may include the number and identity of people who are entitled to use the software as well as the purposes for which they are entitled to use it. Misuse of the software will typically disentitle the customer from relying on its protections elsewhere in the agreement, such as warranties and service credits, and the customer should therefore ensure that its intended use is consistent with the permitted uses allowed by this clause.

2. Service Levels

Unlike in traditional software licensing arrangements, where software is installed on the customer's computer, SaaS arrangements require the customer to access software remotely. As a result, customers are reliant on the supplier's network infrastructure and its ability to prevent and swiftly resolve technical issues. It is therefore critical that the customer sets clear expectations by specifying service levels for the availability of the software and the time taken to respond to and fix problems.

Further, a customer may struggle to prove that the damages it is seeking were caused by the supplier's failure to reach the service levels. To deal with this the customer should request a pre-defined financial remedy — often referred to as liquidated damages — for a failure to meet the service levels. While these will often be in the form of service credits, customers should ensure that this is not their sole remedy and that damages can be sought for a wider range of losses.

3. Support and Maintenance

Customers will typically need to provide certain technical support services and maintenance in order to use the software effectively. For software that is critical to their daily business operations, customers should seek comprehensive and detailed specifications of the support that will be provided.

4. Data Sovereignty

The location of data stored by suppliers under SaaS contracts will have critical jurisdictional implications. Customers should seek to keep their data in Australia for two key reasons:

- As a practical matter, ensuring that data is stored only in one specified place reduces the number of points at which unauthorised access to their data can occur.
- The Australian Privacy Principles, which are a set of guidelines designed to uphold compliance with the Privacy Act, forbid transfer of data to a country without ensuring that the data will receive substantially similar protection after that transfer to that which it would receive if located in Australia. To comply with this, customers should insist on clauses which require the supplier to store their data in Australia, and which prohibit the transfer of the data to a foreign jurisdiction.

5. Data Security

A major consideration for customers in SaaS agreements should be the security and protection of their data. There are four key clauses which will assist customers in upholding high security standards and, in the event that a security incident does occur, seeking an appropriate remedy:

- A general requirement that the supplier comply with recognised security standards. The International Organisation for Standardisation ('ISO') produces a recognised security standard for cloud services called the ISO 27017 which is reviewed every five years. If the customer does not have its own security standards to impose, customers should require compliance with the ISO's standard.
- A list of minimum preventative measures which the supplier must take to minimise the risk of a security incident occurring. This will allow the customer to add any specific measures which exceed the relevant security standard.
- An obligation on the supplier to notify the customer as soon as it is aware of a potential security incident. This will allow the customer to monitor and appropriately manage the incident.
- An obligation on the supplier to take certain measures in response to a security incident. Typically, these will be obligations to investigate, diagnose, manage, and contain the incident and to make adjustments to the supplier's practices to prevent future incidents.

6. Supplier Use of Customer Data

Customers need to protect their data not only against third party security incidents but also against misuse by the supplier. Data is an increasingly valuable commodity and customers therefore need appropriate safeguards to prevent the data being sold or otherwise misused for the supplier's purposes. There are three aspects to constraining the supplier's use of customer data:

- An obligation to use the data only for permitted purposes ('permitted purpose clause'). Typically, the permitted purposes will be the provision of services, or compliance with obligations, under the agreement.
- An obligation to handle the data in a way that prevents it from being accessed by persons beyond the supplier's control who are not bound by the terms of the agreement ('restricted access clause'). This ensures that any person handling the data is bound by the permitted purpose clause.
- An obligation to delete the data upon termination of the agreement ('data deletion clause'). Much like the restricted access clause, a data deletion clause ensures that no person has access to the data unless they are bound by the permitted purpose clause. It is critical to preventing misuse of the data after the agreement, including the permitted purpose clause, has ceased to bind the supplier. Many of the recent high profile data breaches in Australia involve unauthorised access to data that the supplier is no longer using. Because the data is old, the supplier might not keep it as securely as current data and so the data is more easily accessed by a data hacker.

7. Customer Rights to Access Data

For several reasons, customers should ensure that they have a right to access their data at all times during the agreement's term:

- During the course of the agreement, the customer may wish to withdraw its data so as to prevent it from being lost or damaged in the supplier's possession.
- If the customer wishes to seek the services of another supplier, it will need to transfer the data onto the new supplier's platform.
- This provision will allow the supplier to exercise properly its ownership of the data by retaining possession and control of it.

8. Privacy

A supplier may also come into contact with personal information which does not belong to the customer. Customers should seek to ensure that personal information of this kind is treated under the agreement in much the same way as its own data would be.The data must therefore be stored within Australia's jurisdiction, comply with the Privacy Act, be handled according to appropriate security standards and security incidents must be appropriately prevented, managed and remedied.

A related issue is confirming whether the customer does in fact have the right to transfer third party (such as the customer's own customers) personal information to the cloud supplier. The use of cloud suppliers to process third party information should be clearly disclosed in the customer's own privacy policy.

9. Third Party Intellectual Property Rights

Customers should therefore seek a warranty that the customer's use of the cloud service will not expose it to any claims for infringement of third party intellectual property rights and a full indemnity against any claims made by third parties on the basis of those rights. Customers may also wish to impose an obligation on the supplier to manage any negotiations and defend any proceedings arising out of a third party claim.

10. Fees and Payment

Software markets are competitive and fast-paced. Customers in strong bargaining positions ought therefore to ensure flexibility in setting the price of the software service. One effective strategy is to use a benchmarking clause. The benchmarking clause requires the price of the software service to be compared with comparable providers in the Australian market by an independent benchmarker. The parties will often then be invited to agree upon a reduction in the price that fairly reflects the benchmarker's report. This prevents customers from being trapped in uncompetitive supply arrangements.

Another option is to enter into short term supply arrangements, so that the customer is free to decide at the end of the term whether to continue with the current supplier or to obtain services from someone else.

11. Termination, Suspension and Transitions

As described above, customers need to maintain as much flexibility as possible to seek out the most competitive software services available. Buyers in a strong bargaining position should seek broad termination rights including termination for cause and for convenience. At times, the customer may wish to suspend the services during periods where they are unnecessary without fully terminating the agreement. In this case, customers should seek to avoid making ongoing payments for the services and, as a compromise, accept liability for all reasonable costs to the supplier arising from the suspension.

Transition-in and -out plans can also be useful devices to help with transferring services from one supplier to another. The supplier should be required to agree upon specified obligations and rights to apply during the transfer period. These plans may require a supplier to co-operate with the customer or with other suppliers to maintain supply and minimise the impact of transitions to other software providers, as well as attending to management of data, records and other property.

12. Survival of Obligations

Since data and information protection is a key consideration for customers in SaaS agreements, the need to ensure that the supplier adheres to the terms of the agreement does not vanish upon termination of the agreement. To the contrary, once the business relationship has ended, customers will need to know that their data and personal information is treated with care. Customers should therefore list the key protective provisions of the agreement that survive its termination in a separate clause. In particular, provisions relating to protection of data, privacy, protection of personal information, insurance and confidentiality should survive termination, however that termination is effected. As mentioned above, it is also important to include a provision requiring the supplier to delete upon termination all customer data that it hold.