PREPARED BY

GalkinLaw

internet law · new media law · technology law

The 10 KEY ISSUES FOR SAAS AGREEMENTS

GOT QUESTIONS ABOUT SAAS AGREEMENTS?

CONTACT US FOR A FREE CONSULTATION AT

WWW.GALKINLAW.COM | INQUIRIES@GALKINLAW.COM | (410) 484-2500

THE 10 KEY ISSUES FOR SAAS AGREEMENTS

INTRODUCTION

A Software as a Service (SaaS) agreement is a hybrid of a service and license agreement. SaaS is a service in that functionality is provided to the Customer. However, SaaS is also considered a license because the functionality involves the remote operation of software. So, is a SaaS agreement an agreement for services or software? Well, it's both.

The 10 Key Issues for SaaS Agreements below are discussed in the context of agreement clauses. The topics of the referenced clauses are found in many agreements and all the nuances or variations of these clauses are beyond the scope of the discussion in this document. Instead this document focuses on the unique issues a SaaS offering raises that impact these agreement terms.

1. LICENSE SCOPE

a. The license scope defines how the system can be used by the Customers. Licenses are by definition limiting (as opposed to ownership that is unlimited). A Customer can only use the system for a use that is within the defined scope.

b. From a Provider's perspective, scope is structured to maximize revenue. Therefore, scope should be scalable, getting more expensive as the scope expands.

c. Scope parameters are linked to functionality and use. For example, parameters can include number of users, vectors, email boxes, transactions, locations, entities, business units, countries, vehicles, fields of use, etc. In order to model a license scope, Providers need to carefully think through their business model.

d. From a Customer's perspective, the scope must include all intended uses and scenarios. The last thing a Customer wants is to receive a notice that the license scope has been violated, and more license fees are due. For instance, a Customer may intend to allow multiple affiliates to use the system. A standard license grant is only to the signing Customer entity, so affiliate use would need to be specifically called out.

e. Standard license scope limitations to consider include: internal use only, no service bureau use, and user personnel only.

f. License scope restrictions should include: no reverse engineering (not so relevant for SaaS but there are some circumstances where this could be relevant), no service bureau usage, and no publishing of benchmarking results.

g. Providers will want a right to audit a Customer's use to verify compliance with the license. Also, an agreement should be explicit that the system may also perform such monitoring and will enforce license scope and restrictions.

2. LICENSE FEES

a. Licenses can be payable in advance or in arrears. Payments in arrears would apply under circumstances where the license fee is linked to a metric that can vary each month (like number of transactions or revenue throughput). Even when fees are payable in arrears, a Provider would be wise to consider charging an estimated or minimum fee in advance, subject to true up.

b. Many Providers miss the opportunity to charge a set up/implementation fee. This fee can always be waived when appropriate – which will win points with the Customer.

c. Providers will prefer fees payable annually in advance, whereas Customers would normally prefer monthly or quarterly advance fee payments. A Provider may incentivize longer upfront payment terms by making such payments subject to a discount.

d. If there are implementation services required prior to going live, then the issue arises as to when license fees begin to be paid. A Provider can justify asking for payments to begin upon license execution because maintenance becomes active at that time and maintenance is an ongoing cost that benefits the Customer from day one. Of course, the Customer can argue otherwise.

e. Price protection imposes a limit on how much and when a Provider can increase the subscription fee. Providers will often seek to leave price increases without limit. However, a savvy Customer will seek to lock in the fee for a number of years and then limit the increases to a set percentage, CPI, or a combination (CPI + X%). Whether price caps are critical for a Customer will depend upon considerations such as (1) how critical is the system to the Customer's business, (2) whether there are comparable alternatives, and (3) how long will it take to transition to a substitute system.

3. LICENSE TERM

a. SaaS license terms are all limited by definition (as opposed to installed software that can be subject to a perpetual license). A standard term would be for 12 months, renewal for subsequent 12-month terms.

b. Though a standard initial term is 12 months, a Provider or Customer may want the initial term to be longer. For the Provider, a longer initial term may represent an extended revenue guaranty, subject to termination for convenience rights of a Customer. For the Customer, a longer initial term offers stability as to the system. A Provider may also require a longer initial commitment to cover initial sales, onboarding and implementation costs.

c. Renewals can be automatic, subject to either party's right to terminate upon prior notice, not automatic and always subject to mutual agreement, or at the Customer's option. Provider's prefer automatic renewals and Customer's may be indifferent or not to automatic renewals.

d. On occasion, a Customer may require the right to renew the license at its option. This would be the case for a mission critical system. Under normal circumstances, Providers can accept this, but the option period should be reasonably limited, so that the Provider has flexibility in case of unforeseen circumstances.

e. Many Customers will ask for a termination for convenience right. The Provider's business model will determine the Provider's position on this. Many Provider's fight against a termination for convenience right, and if they give in, it's combined with a required payment of a termination for convenience fee.

4. SERVICE LEVELS

a. **Service levels can apply to**:

   i. System uptime
   ii. System response time
   iii. Maintenance response

b. ***System uptime*** is measured by a percentage. Uptime guaranties of less than 99.7% are not common these days. Downtime can result from factors in the Provider's control and factors not in the Provider's control. Unless the Provider has its own servers, downtime may be caused by the third-party hosting provider – which is not in the Provider's control. However, downtime can also be caused by the Provider's applications. In each case, the system is down and the Customer will not care what the cause is.

c. **Maintenance response** may be measured by how long it takes the Provider maintenance staff to respond to a support request or by the amount of time that elapses between a Customer problem report and the implementation of the solution. Response solution times will vary by the criticality of the support issue.

d. ***System response time*** is measured by the amount of time it takes the Provider's system to perform a function. This requires a complex analysis to arrive at an accurate measuring process (taking into account outside variables, like Internet performance). Therefore, this service level will rarely be implemented except for mission critical and heavy investment implementations.

e. Failure to meet a service level may or may not result in a credit or penalty. If there is no credit or penalty, then the consequences will be customer dissatisfaction or termination for breach. Failure to meet a response or resolution target should at a minimum be subject to escalation to Provider management. An uptime guaranty is the easiest service level for application of a credit or penalty – because it is easily measurable, assuming that the Provider actually measures availability. Credits can also apply to a failure of maintenance response or resolution. Response times are usually easy for a Provider to meet, but resolution times are not predictable and therefore associated credits will often be resisted by Providers. If a credit applies, then the Provider will usually want to limit the amount to a percentage of the monthly equivalent fee.

5. DATA SECURITY/PRIVACY

a. Data security terms cover systems, procedures and consequences relating to data breaches. This is the hot issue today for many Customers. However, it's not all under the control of the Provider. What's more, the reputational and financial consequences of data breaches can be substantial. Since data breaches occur all day every day – it's not a theoretical issue and must be managed by both sides.

b. A data protection provision will begin with a commitment to data protection, and should include reference to a Provider or Customer security policy. If a Customer makes subsequent changes to its security policy, then the obligation of the Provider to comply needs to be considered. A wise Provider will pre-empt this issue by offering upfront its security policy. The Customer will then be responsible for evaluating the adequacy of the Provider's policy.

c. However, rubber hits the road around the issue of who bears the liability for a data breach. The resulting liability could be a combination of compliance with state data breach laws (notification, identity theft protections), loss to business and reputation, and customer or shareholder lawsuits. Each of the foregoing liabilities can be substantial. Who will be liable?

d. Before we get there, Providers and Customer need to get and review insurance that covers liability for data breaches. This type of insurance is no longer a luxury or exotic and should be considered a necessity.

e. When evaluating this issue, it's necessary to drill down and determine what consumer, sensitive, protected information is held on the Provider's servers. Sometimes there is virtually none and the battle of liability can be completely avoided.

f. Liability will be covered in the agreement in two ways (1) determining whether the Provider or Customer is responsible for compliance with state data breach laws, and (2) including data breach liability under an indemnification.

g. The negotiation on these issues can go in many directions, arguments can be raised on both sides, and multiple compromises can be reached. So, it's important going in that a Provider and Customer have clear positions to present and know where they can give.

7. ESCROW

a. Software escrow provisions will often appear in "installed software" end user license agreements. Escrows are only warranted where the software is mission critical, otherwise the Customer can just transition to a different product.

b. It's much less common for software escrows to be established for SaaS systems for several reasons. First, SaaS systems are almost always for limited terms, so if a source code release is triggered, it typically would only be used for the remainder of the then-current term. Second, in addition to a Customer needing appropriate expertise just to operate the software, the Customer will also need to obtain a proper hardware configuration and implementation – which may itself be a difficult, time consuming, and expensive process. Third, SaaS systems usually operate with multiple third party applications and connectors – which also need to be available upon the occurrence of the agreed escrow release trigger.

c. Nevertheless, escrows are requested in SaaS licenses from time to time. All the standard terms applicable to in bound software licenses would apply. However, the escrow for a deposit for a SaaS system varies from the standard deposit because, as mentioned, in addition to the source code, object code, third party software, connectors and a proper hardware configuration need to be made available.

d. There are some services available that operate a mirrored SaaS system or maintain a configuration that can be activated for this purpose. This allows the SaaS to be up and running quickly (theoretically) and solves the implementation challenge mentioned above. Who pays the escrow cost needs to be considered.

8. WARRANTIES

a. Specific warranties cover issues such as performance, no infringement, and no viruses. The standard warranties are appropriate, such as (1) functionality in accordance with documentation, (2) non-infringement, and (3) no viruses.

b. Providers often want to give no performance warranties for SaaS systems. The argument is that the Customer can test it out in advance and if it does not work the Customer can terminate and get a refund of unused fees, so what's the point of any warranty? However, some SaaS systems are more customized and don't allow for pre-testing.

c. A warranty is more important where the Customer has to pay for implementation, in which case, the Customer would not just want a pro-rata refund, but also a refund of the implementation fees.

d. Additionally, Customers will want some warranty (during the whole term or for a limited period after execution) which demonstrates the commitment of the Provider to the SaaS system performance. Warranty breaches also do give Customers additional remedies than ordinary contract breaches. Therefore, from a Provider's perspective, it's better to give a short warranty on the SaaS service, and then warrant that the maintenance services will keep the system working in compliance with published documentation.

e. Depending upon the SaaS system, it may be critical for the Customer to get a warranty that the system will be updated as necessary to maintain compliance with laws.

f. Often providers of installed software seek to exclude third party products, especially open source software, from the intellectual property indemnification. This is much less of an issue in the SaaS environment, because the Provider is operating the system and will always be primarily liable for infringement resulting from use of the entire SaaS system.

9. INDEMNITIES

a. Indemnities are always a touchy issue. The spectrum can run from no indemnity to everything, like (1) non-infringement, (2) breach of warranties, (3) breach of confidentiality, (4) breach of security, and (5) negligence.

b. Most of these indemnifications can be negotiated in a standard way, based upon each party's risk profiles. However, the area that is unique in the SaaS environment is the indemnification that relates to data security, because unlike under a standard end user license agreement, in a SaaS environment, the Provider may be holding sensitive data that can be breached.

c. Indemnifications can be drafted to cover amounts awarded to third parties or also include internal expenses and costs. Allocation of risk on this issue has been discussed above in the Data Security/Privacy section. However, even if a Provider is agreeing to bear some liability for data breaches, then scope of that liability needs to be clarified and specified in the indemnification. Agreeing to be liable for amounts awarded to a third party is the usual liability. However, agreeing to also be liable under the indemnification for internal (and possibly consequential) damages would be out of the ordinary. So this provision should be carefully reviewed by the Provider.

d. An important distinction to make is between indemnifying for a breach of data security/privacy obligations and indemnifying for the outcome of any data breach incident. It's critical to understand the difference. Indemnifying for a breach of obligations means that if a data breach occurs, and the Provider did not breach its obligations, then there is no liability. On the other hand, indemnifying for the outcome of any data breach incident means that even if the best security was observed, and a hacker nevertheless got it, then there is still liability.

10. LIABILITY LIMITATIONS

a. At the end of the day risk and remedy all come down to the liability limitations.

b. Liability limitations fall into two categories: (i) indirect/consequential/incidental damages (think primarily of lost profit and cost to recover) and (ii) overall liability cap.

c. A standard approach would be to exclude all indirect and consequential damages, and cap liability at some amount that relates to the value of a number of monthly fees (anywhere from 1 to 24 would be in a standard range).

d. The interesting discussions then come around what liabilities are excluded from the above liability limitations. If a Customer does not read this section carefully, they may find that all of the hard earned clauses become worthless if all liability is limited.

e. Common exclusions from the liability limitations to be negotiated include: (1) gross negligence, (2) willful misconduct, (3) breach of confidentiality, (4) breach of security/privacy, and (5) indemnifications. There are many ways to creatively skin the cat on these liability issues.