
# SaaS Agreements

## A Practical Guide

By Bradley J. Freedman

# SaaS Agreements

## A Practical Guide

By Bradley J. Freedman

# Table of Contents

# Introduction

Computer software is an essential tool for almost every organization. Businesses and other organizations use computer software to create products, perform services, manage relationships, control internal operations, and process and store sensitive and regulated data. Almost every organization procures and uses various kinds of computer software and ancillary services provided by numerous software vendors/service providers.

There are two basic business/technology models for the procurement and use of computer software:

- Traditional Installed Software: The traditional installed software model involves the customer using copies of computer software installed and maintained by the customer (or its service providers) on the customer's own technology infrastructure.
- SaaS: The software-as-a-service (commonly known as "SaaS") model involves the customer using its technology infrastructure to remotely access and use copies of computer software installed and maintained by a service provider on the service provider's technology infrastructure.

Each model has distinctive characteristics that affect the rights and obligations of the customer and the software vendor/service provider. Consequently, the contracts used for each model are significantly different. The contract for the traditional installed software model is commonly known as a "software license agreement". The contract for the SaaS model is commonly known as a "software-as-a-service subscription agreement" or a "cloud service subscription agreement". This handbook discusses agreements for the SaaS model, which will be referenced as "SaaS agreements". Software license agreements are discussed in BLG's *Software License Agreements – A Practical Guide, 2nd Edition*.

SaaS agreements can take various forms and be implemented in various ways. Inexpensive and relatively simple SaaS is often governed by a standard form agreement the customer must accept before or during the service registration process. Expensive SaaS that is costly and complicated to implement is often governed by a signed agreement that is subject to negotiation by the service provider and the customer.

The use of SaaS is a form of outsourcing that implicates compliance with legal and regulatory requirements (including laws of general application and sector-specific laws, contractual obligations and legal duties) and can present the customer with significant business risks and legal liabilities, which should be addressed in the applicable SaaS agreement. Consequently, a prudent customer, with the benefit of legal advice, will carefully review each SaaS agreement and attempt to negotiate required revisions so that the agreement is appropriate and reasonable in the circumstances.

This handbook explains some of the important provisions commonly included in SaaS agreements and provides some practical guidance for organizations considering the procurement of SaaS. This handbook provides general information only, and does not constitute legal or other professional advice. Organizations procuring SaaS are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.

**Bradley J. Freedman**
October 2022

# SaaS Procurement

SaaS is a form of cloud computing that enables the customer to outsource some of its computer software and information technology ("IT") requirements to a specialist service provider in the expectation that the service provider will implement, operate and maintain the software and related IT infrastructure in a better and more efficient and cost-effective manner than the customer using its internal IT resources. The term "cloud" is a metaphor for the Internet and an abstraction for the underlying information technologies used by the service provider to operate the SaaS. SaaS can provide both significant benefits and substantial risks to the customer.

## Service and Deployment Models

SaaS makes computer software and related IT resources (e.g., networks, servers and data storage) and ancillary services (e.g., hardware and software maintenance, technical support and problem resolution) available as a utility or consumption-based service. Most SaaS have some or all of the following characteristics: (1) pooled IT infrastructure, software instances and resources used for multiple customers; (2) broad access over the Internet; (3) flexibility (i.e., elastic and scalable to meet a customer's changing requirements); (4) on-demand, self-service provisioning; and (5) fees based on measured usage.

SaaS can be deployed using various IT infrastructure models (e.g., public cloud, private cloud, community cloud and hybrid cloud), reflecting whether and how customers are willing to share IT infrastructure and software instances. The IT infrastructure might be owned and operated by the SaaS service provider or by its subcontractors and service providers.

## SaaS Benefits and Risks

SaaS can provide a customer with potentially significant benefits, including: (1) lower cost and financial risk; (2) flexibility (i.e., elastic and scalable service to meet the customer's changing requirements); (3) agility (i.e., relatively easy and quick access to new technologies as and when required); and (4) improved service quality and customer productivity.

SaaS can also present a customer with potentially substantial risks, including risks relating to: (1) business disruption; (2) the security, confidentiality, integrity and availability of the data processed or stored using the SaaS; (3) compliance with contractual obligations (including confidentiality and data protection obligations); and (4) compliance with applicable laws (including data security and privacy obligations) and legal obligations.

The actual benefits and risks of each SaaS will depend on the particular circumstances, including: (1) the service and deployment models used for the SaaS; (2) the importance of the SaaS to the customer's business operations; (3) the nature and source of the data processed or stored using the SaaS; (4) the character, quality and experience of the service provider; (5) the nature of the customer and its industry sector; (6) the legal rules and requirements applicable to the customer and its operations; (7) the customer's ability to implement controls and other measures to mitigate risk and to timely procure replacement software or services if the SaaS is not available for use by the customer; and (8) the allocation of risk established by the applicable SaaS Agreement.

## Procurement Process

Guidance issued by regulators (including privacy commissioners), self-regulatory organizations and other authoritative sources emphasize that a customer's decision to use SaaS should be based on a reasonable, documented assessment, informed by appropriate due diligence and expert advice, as to whether the relative benefits of using the SaaS justify the relative risks in light of all of the circumstances, including the organization's overall enterprise risk tolerance.

There are many different kinds of SaaS, and each SaaS can be used in different ways for different purposes. Consequently, the risk/benefit assessment of a SaaS should be specific to the SaaS and each intended use of the SaaS. In some circumstances, a specific use of a particular SaaS will be entirely appropriate, while a different use of the same SaaS will not justify the risks.

A risk/benefit assessment of a SaaS should not be limited to IT issues or be prepared solely by IT personnel. The assessment should include risks/benefits to all aspects of the customer's operations and involve the participation of representatives from all of the customer's relevant operational areas. Further, the risks and benefits of a proposed use of a SaaS should be assessed realistically and in comparison with the risks and benefits of practicable alternatives.

The applicable SaaS agreement (including the service provider's promises about the availability and quality of the SaaS, the risk allocation provisions and provisions required for legal compliance) is usually an important consideration when assessing the risks/benefits of using a SaaS. Regulators, self-regulatory organizations and other authoritative sources have issued guidance regarding the provisions that should be in a SaaS agreement.

## Recommendations

A customer's decision to procure and use a SaaS should be based on a thorough and reasonable assessment of the potential benefits and risks of the intended use of the SaaS in light of all circumstances, including the customer's ability to mitigate risk and the risk allocation established by the SaaS Agreement. ■

# The SaaS Subscription

SaaS agreements should give the customer a permission – commonly called a "subscription" – to remotely access and use the SaaS. The subscription usually specifies how the customer may access and use the SaaS, the purposes for which the customer may use the SaaS and other restrictions and requirements.

The SaaS subscription is of primary importance to the customer because use of the SaaS beyond the scope of the subscription is a breach of the SaaS agreement and might constitute an infringement of the service provider's rights in the SaaS. If the customer violates the limits and restrictions specified in a SaaS agreement, then the customer risks serious adverse consequences, including financial liability to the service provider and early termination of the SaaS subscription.

## Permissible Users and Beneficiaries

SaaS agreements usually grant the SaaS subscription to the customer only and prohibit the customer from sharing the SaaS subscription with other persons (including the customer's corporate affiliates and subsidiaries). In addition, SaaS agreements usually prohibit the customer from using the SaaS to provide services to or for the benefit of any other person (including the customer's corporate affiliates and subsidiaries).

## Scope of Use

A SaaS subscription defines the scope of the customer's permissible use of the SaaS. The scope of a SaaS subscription can be adjusted by limiting or restricting various aspects of permissible SaaS use. For example:

- The SaaS: The particular SaaS modules, features or functionalities that may be used under the subscription.
- End-Users: The individuals who may use the SaaS. For example, a SaaS subscription might limit the total number of concurrent individual users of the SaaS, limit use of the SaaS to specific individuals (e.g., identified by name, business role or location), or impose other requirements (e.g., a user must be employed by the customer) or prohibitions (e.g., a user must not be an IT service provider engaged by the customer).
- Purposes: The purposes for which the SaaS may be used. For example, SaaS subscriptions commonly provide that the SaaS may be used for the customer's "internal business purposes only" and prohibit use of the SaaS to provide services to or for the benefit of other persons (e.g., the customer's corporate affiliates or subsidiaries).
- Manner of Use: The way in which the SaaS may be used. For example, a SaaS subscription might limit the number or kinds of systems, software or interfaces that may be used to access or use the SaaS or exchange data with the SaaS, or the kinds and amounts of data that may be processed or stored using the SaaS.
- Location of Use: The locations or geographic territories from which the SaaS may be used.
- Duration of Use: The duration of the subscription. For example, SaaS subscriptions are usually time-limited and subject to suspension or termination in specified circumstances.

## Documentation

SaaS agreements usually give the customer a permission – commonly called a "license" – to reproduce and use technical documentation (e.g., user manuals) regarding the SaaS. Licenses for technical documentation are often subject to the same limits and restrictions that apply to the use of the SaaS.

## Technological Enforcement Mechanisms

Service providers use technological measures to help enforce certain kinds of SaaS subscription restrictions and requirements and prevent unauthorized use of a SaaS. For example, service providers usually require a customer's authorized end-users or data interfaces to use registered credentials (e.g., user names, passwords and other unique identifiers) to remotely access a SaaS. In addition, SaaS agreements usually allow the service provider to monitor the customer's use of the SaaS to verify compliance with the SaaS subscription.

## Contractual Enforcement Mechanisms

Some kinds of SaaS subscription restrictions and requirements cannot be enforced by technological measures. The service provider must rely on contractual enforcement mechanisms – monitoring, periodic reports and audits – to detect breaches of the restrictions and requirements.

Some SaaS agreements require the customer to pay punitive fees for all unauthorized use of the SaaS that is discovered by the service provider using contractual enforcement mechanisms. Consequently, the customer should take steps (including educating the customer's employees and conducting internal audits) to prevent unauthorized use of the SaaS.

## Changes

Some SaaS agreements permit the customer to change the scope of the SaaS subscription, subject to specified minimums. For example, the customer might be permitted to increase the maximum number of end-users of the SaaS or the amount of data processed or stored using the SaaS. Those kinds of provisions enable the customer to adjust the SaaS subscription, at a predetermined cost, to accommodate changes to the customer's business requirements.

## Recommendations

When negotiating a SaaS agreement, the customer should ensure that the SaaS agreement allows the customer and its corporate affiliates and subsidiaries (if applicable) and service providers (if appropriate) to use and benefit from the SaaS as required for current and reasonably anticipated future needs. The customer should also take reasonable precautions to minimize the risk of unintentional use of the SaaS and documentation in breach of the SaaS agreement. ■

# SaaS Availability and Quality Promises – Warranties and Disclaimers

SaaS agreements often contain limited promises by the service provider regarding the availability and quality of the SaaS, and provide limited remedies for the customer if the SaaS is deficient. The customer should understand those provisions and manage and mitigate risk through other contractual rights and prudent business practices.

## SaaS Availability Promises

SaaS agreements often include limited promises (sometimes called a "service level agreement" or "SLA") by the service provider about the availability of the SaaS for use by the customer. For example, service providers often promise that their SaaS will be available for use by the customer not less than a specified percentage of time (e.g., not less than 99.99%) measured over a specified period (e.g., each month) throughout the term of the SaaS subscription. In addition, some SaaS agreements require the service provider to deliver to the customer periodic reports regarding SaaS availability.

SaaS availability promises are usually limited to the customer's ability to use the SaaS, and do not include promises about the quality (i.e., functionality, operation, performance and results) of the SaaS. In addition, SaaS availability promises are usually subject to various exclusions (e.g., scheduled and emergency maintenance) and exceptions for downtime caused by the customer's breach of the SaaS agreement or circumstances beyond the service provider's control.

SaaS agreements often provide the customer with limited remedies (e.g., credits against future fees payable by the customer and termination of the agreement in limited circumstances) if the SaaS fails to comply with availability promises and the customer submits a timely claim using a prescribed procedure. The limited remedies might be exhaustive and expressly exclude all other remedies, including financial compensation for loss and damage suffered by the customer as a result of the inability to use the SaaS or a right to terminate the SaaS agreement.

## SaaS Quality Warranties

Some SaaS agreements contain limited promises (known as "warranties") by the service provider regarding the quality (i.e., functionality, operation, performance and results) of the SaaS. For example, the service provider might promise that the SaaS will conform to the description in the applicable documentation or comply with specified performance metrics. SaaS quality warranties are usually subject to exceptions for problems caused by the customer (e.g., the customer's improper configuration or use of the SaaS or the customer's failure to use compatible infrastructure to access the SaaS) or by circumstances beyond the service provider's control.

SaaS agreements usually provide the customer with limited remedies if the SaaS fails to comply with the quality warranties and the customer submits a timely claim using a prescribed procedure. For example, the service provider might be required to either correct the problem or terminate the customer's SaaS subscription and refund the unused portion of pre-paid fees for the terminated subscription. The limited remedies for breach of quality warranties are usually exhaustive and expressly exclude all other remedies, including financial compensation for loss and damage suffered by the customer as a result of the defective SaaS.

## Disclaimers

SaaS agreements usually contain detailed provisions (known as "disclaimers") that exclude all other promises regarding the availability and quality of the SaaS. Disclaimers often provide that the express availability and quality warranties in the SaaS agreement are in place of all other promises regarding the SaaS, including promises that might otherwise be implied by law. In addition, disclaimers often specify that the customer is solely responsible for selecting the SaaS and determining the suitability of the SaaS for the customer's particular purposes.

## Entire Agreement Clause

SaaS agreements often supplement disclaimers with a provision (known as an "entire agreement" clause) that confirms that the SaaS agreement supersedes and replaces all prior discussions, promises, understandings and agreements between the service provider and the customer regarding the SaaS. An entire agreement clause is intended to prevent either party from relying on pre-contractual discussions or assurances (including statements in the service provider's advertising and marketing materials and commitments made by the service provider during sales presentations and negotiations) that are not confirmed in the SaaS agreement.

## Recommendations

Limited availability promises, warranties and disclaimers usually restrict the customer's rights and remedies if the SaaS is not available for use by the customer, or is defective or otherwise fails to meet the customer's specific requirements. When negotiating a SaaS agreement, the customer should ensure that the SaaS agreement: (1) accurately confirms all of the commitments made by the service provider during sales presentations and due diligence investigations; and (2) provides the customer with reasonable and appropriate rights and remedies if the service provider breaches those commitments. The customer should also manage and mitigate risk through prudent business practices (e.g., pre-contractual due diligence and business continuity planning). ■

# Acceptance Testing

Some SaaS agreements prescribe a procedure known as "acceptance testing", which allows the customer to verify that the SaaS meets specified requirements. The importance of acceptance testing will depend on the circumstances, including the customer's ability to test or evaluate the SaaS before purchasing a SaaS subscription, the extent to which the SaaS must be implemented (configured or integrated) by or on behalf of the service provider for use by the customer, the cost of the SaaS subscription and the customer's legal and practical ability to terminate the SaaS agreement if the SaaS is deficient.

## Testing Procedure

Acceptance testing provisions usually specify one or more limited periods during which the customer may test the SaaS to determine whether the SaaS meets specified requirements. Depending on the circumstances, acceptance testing might occur not only when the SaaS is initially made available to the customer but also after the SaaS is implemented.

In some circumstances, acceptance testing is a collaborative process in which the service provider assists the customer to conduct the testing. The customer is usually required to give the service provider detailed notice of all deficiencies in the SaaS identified by the customer during testing, and allow the service provider a reasonable opportunity to correct the deficiencies and make the SaaS available for further testing. The customer is also usually required to give the service provider prompt written notice if the SaaS passes or fails acceptance testing. SaaS agreements often provide that the SaaS is deemed to pass acceptance testing if the customer does not give timely notice that the SaaS has failed acceptance testing.

## Acceptance Criteria

Acceptance testing provisions often specify criteria – known as "acceptance criteria" – for the customer's acceptance or rejection of the SaaS. For example, the acceptance criteria might be the standard functionalities of the SaaS described in the SaaS documentation. In appropriate circumstances, the customer might also require that the acceptance criteria include detailed specifications (e.g., required functionalities, operations, performance and results) that reflect the customer's particular requirements.

Acceptance testing provisions often provide that the SaaS will pass acceptance testing if the SaaS "substantially conforms" to the acceptance criteria. However, that approach might not be appropriate in all circumstances, particularly if the customer expects and requires that the SaaS comply with all acceptance criteria.

## Consequences

Acceptance testing provisions usually specify the consequences or remedies for successful acceptance testing and acceptance testing failure. For example, successful acceptance testing might constitute a payment milestone. On the other hand, acceptance testing failure might give the customer an option to either terminate the SaaS subscription and receive a refund of pre-paid fees, negotiate revisions to the acceptance criteria and a corresponding fee adjustment, or give the service provider more time to correct identified deficiencies so that the SaaS passes acceptance testing.

## Recommendations

Acceptance testing can be an important way for a customer to manage risk. If a SaaS is subject to acceptance testing, then the SaaS agreement should specify a commercially reasonable acceptance testing procedure, acceptance criteria and the consequences of successful acceptance testing and acceptance testing failure. ■

# Technical Support and Problem Resolution

SaaS agreements usually require the service provider to perform important ancillary services regarding the SaaS, known as "technical support" and "problem resolution", which are essential for the customer's effective use of the SaaS. The customer should understand the nature and extent of the ancillary services, and ensure that the services, together with other risk-management practices, will reasonably satisfy the customer's requirements.

## Services

Technical support usually consists of online information and remote (telephone or online) technical advice regarding the customer's use of the SaaS. Problem resolution usually consists of remote (telephone or online) technical advice and assistance to help resolve certain problems with the SaaS. Technical support and problem resolution might include a help desk service for the customer's end-users of the SaaS (known as "first-level" support) or be limited to assistance to the customer's own internal help desk personnel (known as "second-level" support).

## Service Levels and Remedies

Some SaaS agreements contain limited promises (sometimes called a "service level agreement" or "SLA") by the service provider about how quickly the service provider will respond to and resolve problems with the SaaS. The promised service level often varies depending on the severity of the reported problem.

Some SaaS agreements provide the customer with limited remedies (e.g., credits against future fees payable by the customer and termination of the agreement in limited circumstances) if the service provider fails to provide the promised level of service. Usually, the remedies must be claimed by the customer within a limited period and using a specified procedure. The limited remedies are usually exhaustive and expressly exclude all other remedies, including financial compensation for loss and damage suffered by the customer.

## Exclusions/Qualifications

The service provider's obligations to provide technical support and problem resolution services are usually limited by various exclusions and qualifications. For example, the SaaS agreement might limit technical support and problem resolution to problems that can be replicated by the service provider and exclude problems caused by use of the SaaS in breach of the SaaS agreement or contrary to applicable documentation.

## Recommendations

Technical support and problem resolution services are particularly important for SaaS that is essential to the customer's daily business operations and difficult to replace promptly. In those circumstances, the customer should ensure that the service provider's obligations regarding technical support and problem resolution, together with the customer's other risk-management practices, will reasonably satisfy the customer's requirements throughout the entire period that the customer expects to use the SaaS. ■

# Fees and Related Matters

SaaS agreements usually require the customer to pay fees for the SaaS subscription and ancillary services. The customer should ensure that the SaaS agreement provides certainty regarding the customer's total cost of using the SaaS throughout the entire term of the agreement.

## Kinds of Fees

A SaaS agreement might require the customer to pay various fees, including subscription fees, data processing/storage fees, fees for ancillary services, and fees for optional professional services.

The fee for a SaaS subscription usually reflects the value the customer expects to derive from using the SaaS, based on the duration and scope of the subscription. SaaS subscription fees might be fixed (i.e., calculated and payable regardless of the customer's actual use of the SaaS), variable (i.e., calculated based on the customer's actual use of the SaaS), or comprised of fixed and variable components. A SaaS agreement might give the customer an option to periodically adjust the scope of the subscription (e.g., adding additional end-users or interfaces or rebalancing other usage metrics) by paying additional specified subscription fees, either in advance or in arrears following a prescribed true-up procedure.

The fee for ancillary services (i.e., technical support and problem resolution) might be included in the SaaS subscription fee or it might be a separate fee calculated using a formula based on the subscription fee.

Service providers usually charge fees for optional professional services, such as SaaS configuration/implementation and training. The fees are often based on a specified fee schedule or calculated on a time and materials basis using the service provider's specified hourly rates (which might be subject to a negotiated discount).

## Fee Increases

Most SaaS service providers change their fees periodically to adjust for inflation and changes in market conditions. SaaS agreements usually limit the service provider's ability to increase fees during the term (including renewals and extensions) of the SaaS subscription, which can be particularly important to the customer if the customer expects to use the SaaS for a lengthy period.

## Taxes and Withholdings

SaaS agreements usually require the customer to pay all applicable taxes on all amounts paid by the customer under the agreement. SaaS agreements often require the customer to pay all fees in full without any withholding or deduction, and include a provision (known as a "tax gross-up") that provides that, if the customer is required by law to make a withholding or deduction from any payment to the service provider, the customer will make an additional payment so that the total amount received by the service provider (net of withholdings and deductions) is the full amount of the required payment.

## Enforcement

SaaS agreements usually allow the service provider to suspend or terminate the SaaS subscription if the customer fails to make a required payment. However, most SaaS agreements include procedural requirements (e.g., a reasonable opportunity for the customer to make the payment after notice of default) to protect the service provider and the customer against the risks of inadvertent administrative errors.

## Recommendations

The customer should ensure that the SaaS agreement: (1) provides certainty regarding the customer's total cost of using the SaaS – all subscription fees (including fees for additional usage rights purchased by the customer from time to time) and fees for ancillary services – throughout the entire period that the customer expects to use the SaaS; and (2) allows the customer a reasonable opportunity to cure any inadvertent breaches of payment obligations before the service provider suspends or terminates the subscription. ■

# Customer Data and Information

SaaS agreements usually include provisions regarding the data/information that will be processed and stored by or on behalf of the customer using the SaaS. The customer should ensure that the provisions reasonably protect the customer's important business interests and are sufficient for compliance with legal requirements, regulatory guidance and recommended best practices. The customer should also manage and mitigate data/information risks through prudent business practices and insurance.

## Data/Information

SaaS is invariably used by or on behalf of a customer to process and store various kinds of data/information, including: (1) personal information about the customer's employees, clients/customers and other individuals; (2) confidential information of other persons and entities; and (3) the customer's sensitive information and other data required for the customer's day-to-day operations.

The processing and storage of data/information in a SaaS might be regulated by laws of general application (e.g., personal information protection and privacy laws) and sector-specific laws (e.g., laws regarding financial institutions, investment industry participants, health care organizations and government agencies), and subject to express or implied confidentiality obligations owed by the customer to other persons and entities. In addition to legal compliance considerations, there are compelling business reasons for a customer to ensure that SaaS agreements adequately address the security, confidentiality, integrity and availability of the data/information processed and stored by or on behalf of the customer using the SaaS.

In most circumstances, the customer is considered to have legal control over, and primary responsibility and liability for, the data/information processed and stored by or on behalf of the customer using the SaaS. However, some laws (e.g., personal information protection laws) impose obligations and liabilities directly on the service provider regarding the data/information processed and stored using the SaaS.

## Specific Provisions

Compliance with legal requirements, obligations and duties to third parties, and recommended best practices usually requires that SaaS agreements include specific provisions regarding the data/information processed and stored using the SaaS. For example, provisions addressing the following issues:

- Data Ownership/Control: The customer's sole ownership of, and legal control over, all data/information processed and stored using the SaaS.
- Data Access: The customer's ability to access and efficiently retrieve all data/information, in specified formats, stored using the SaaS both during and after the term of the SaaS subscription.
- Data Handling by Service Provider: The purposes for which the service provider may access, use and disclose data/information processed and stored using the SaaS, including the service provider's ability to create, collect, use and disclose aggregated or depersonalized data and metadata (i.e., data about the use of the SaaS).
- Consents/Licenses: The customer's obligation to obtain consents and permissions from all relevant persons (including the customer's employees, clients and business partners) required for the lawful processing and storage of the data/information using the SaaS and the handling of the data/information by the customer and the service provider as contemplated by the SaaS agreement.
- Data Locations: The geographic locations where data/information will be processed and stored (including data backups) using the SaaS and where the service provider will perform ancillary services involving the processing or storage of data/information.

- Data Segregation: The service provider's obligation to segregate the customer's data/information from the data/information of other customers or the service provider itself.
- Safeguards: The physical, administrative and technological safeguards the service provider will use to protect the security, confidentiality, integrity and availability of data/information processed and stored using the SaaS.
- Data Incidents: The rights and obligations of the service provider and customer regarding incidents that affect the security, confidentiality, integrity or availability of data/information processed or stored using the SaaS.
- Data Deletion: The service provider's obligation to securely delete all data/information stored using the SaaS at any time on request by the customer and when the SaaS subscription ends.
- Disclosure Demands: How the service provider will respond to legally binding demands (e.g., subpoenas or warrants) from third parties (e.g., government agencies and law enforcement) for disclosures of data/information processed or stored using the SaaS.
- Individual Requests: How the service provider will respond to requests by individuals for access to, information about, or deletion of their personal information processed or stored using the SaaS or used by the service provider to perform ancillary services.
- Monitoring: The customer's ability to monitor (including through required periodic reports, audits/inspections and disclosure of independent audit reports) the service provider's compliance with its obligations regarding data/information.
- Regulatory Audits: Regulators' ability to conduct audits/inspections regarding the SaaS and the processing and storage of data/information using the SaaS.
- Subcontracting: The service provider's engagement of subcontractors and service providers (e.g., providers of cloud infrastructure and platforms) to assist the service provider to operate the SaaS and perform ancillary services involving the processing or storing of data/information.
- Assessments: The customer's ability to conduct periodic legal compliance and risk assessments (including privacy impact assessments) relating to the SaaS.
- Legal Changes: The parties' ability to amend or terminate the SaaS agreement if required for compliance with changes in applicable laws relating to data/information.

## Confidentiality Obligations

SaaS agreement provisions regarding data/information are often supplemented with provisions regarding each party's use and protection of the other party's confidential information. Those provisions should be consistent and drafted to avoid uncertainty about the parties' rights, obligations and liabilities.

## Recommendations

The customer should ensure that the SaaS agreement includes provisions regarding data/information that reasonably protect the customer's important business interests and are sufficient for compliance with legal requirements, regulatory guidance and recommended best practices. The customer should also manage and mitigate data/information risks through prudent business practices (e.g., data backups, business continuity plans, and risk allocation provisions in contracts with potential third-party claimants) and insurance for residual risk. ■

# General Indemnity

SaaS agreements often include a provision – known as a "general indemnity" – that requires a party (usually the customer, but sometimes also the service provider) to protect the other party against certain kinds of claims by third parties and resulting liabilities to third parties. The customer should understand the burdens and benefits of general indemnity provisions and manage risk through prudent business practices and insurance for residual risk.

## Purpose of Indemnity

A general indemnity is a means of contractually allocating the risk of claims by persons who are not parties to the SaaS agreement (known as "third parties") against the contracting parties. The risk allocation can be based on fault (e.g., risk is assigned to the party whose acts or omissions caused the third-party claim), efficiency (e.g., risk is assigned to the party who is best able to manage or control the risk of the third-party claim) or other considerations.

A general indemnity usually imposes two distinct obligations on the indemnifying party for the benefit of the other party and specified other persons (each a "beneficiary"): (1) an obligation to defend the beneficiary against third-party claims, including paying legal costs of defending the claim; and (2) an obligation to indemnify (pay or reimburse) the beneficiary against obligations and liabilities (including court judgments and settlement amounts) resulting from third-party claims.

## Scope of Indemnity

The scope of a general indemnity can be adjusted in various ways, including the following:

- Beneficiaries: The indemnity might be for the benefit of a party only or might also benefit the party's personnel (e.g., directors, officers and employees) or other related persons (e.g., affiliates/subsidiaries, service providers and subcontractors).
- Covered/Excluded Claims: The indemnity might be limited to certain kinds of third-party claims (e.g., claims for bodily injury or damage to tangible personal property), third-party claims resulting from specified events (e.g., the indemnifying party's breach of contract or willful misconduct) or third-party claims made in specified countries.
- Excluded Claimants: The indemnity might exclude claims by certain third parties (e.g., a beneficiary's affiliates/subsidiaries or customers).
- Time Restriction: The indemnity might apply only during the term of the agreement, or it might continue to apply after the agreement ends.

A general indemnity is usually subject to exclusions for third-party claims and liabilities resulting from the beneficiary's breach of the agreement or other specified misconduct.

## Financial Limits

A general indemnity might be subject to limits on the indemnifying party's financial obligations (i.e., legal fees paid to defend third-party claims and amounts paid to settle or satisfy resulting liabilities) under the indemnity. For example, there might be a limit on the indemnifying party's financial obligations in respect of each third-party claim and an aggregate limit on the total amount of the indemnifying party's financial obligations in respect of all third-party claims. A general indemnity might also specify different financial limits (or no limit at all) for different kinds of third-party claims. The limits might be specified in the general indemnity provisions or other provisions that limit or exclude the contracting parties' liability under the SaaS agreement.

## Procedural Requirements

A general indemnity usually requires the beneficiary to comply with specified procedural requirements regarding each third-party claim for which the beneficiary seeks indemnity, such as giving prompt notice of the claim to the indemnifying party, allowing the indemnifying party to control the defence and settlement of the claim, and reasonably assisting the indemnifying party to defend and settle the claim. A beneficiary's failure to comply with procedural requirements might preclude the beneficiary from claiming the benefits of the general indemnity.

## Other Considerations

A general indemnity can be drafted broadly to indemnify the beneficiary for its own damage and loss. Those kinds of broad indemnity provisions (known as "first-party indemnification") can significantly affect the allocation of risk between the parties, and should be carefully considered.

Many SaaS agreements either do not contain any general indemnity by the service provider for the benefit of the customer, or contain a general indemnity by the service provider for the benefit of the customer that is much narrower (in scope and limits) than the general indemnity by the customer for the benefit of the service provider. Whether differences between general indemnities are reasonable and appropriate will depend on the nature of the SaaS and other circumstances.

## Recommendations

When negotiating a SaaS agreement, the customer should understand the burdens and benefits of the general indemnities included (or omitted) in the agreement, and should manage and mitigate risk through prudent business practices (e.g., administrative practices and procedures to minimize risk, and risk allocation provisions in contracts with potential third-party claimants) and insurance for residual risk. ■

# IP Infringement Indemnity and Remedies

SaaS agreements often include a provision – known as an "intellectual property ("IP") infringement indemnity" – that requires the service provider to defend and indemnify the customer, and provide additional remedies, if a third party claims that the customer's use of the SaaS infringes the third party's intellectual property rights. The customer should understand the limited protections and remedies provided by an IP infringement indemnity, and consider procuring insurance for residual risk.

## IP Infringement Indemnity

An IP infringement indemnity provides the customer with limited protection against claims by persons who are not parties to the SaaS agreement (known as "third parties") that the customer's use of the SaaS or related documentation infringes the third party's intellectual property rights (e.g., copyright, patents and trade secrets). An IP infringement indemnity usually imposes two distinct obligations on the service provider for the benefit of the customer and related persons (each a "beneficiary"): (1) an obligation to defend the beneficiary against IP infringement claims, including paying legal costs of defending the claims; and (2) an obligation to indemnify (pay or reimburse) the beneficiary against obligations and liabilities (including court judgments and settlement amounts) resulting from IP infringement claims.

The scope of an IP infringement indemnity can be adjusted using the same variables – beneficiaries, covered/excluded claims, excluded claimants and time restriction – that apply to a general indemnity. An IP infringement indemnity can also be subject to financial limits or caps.

An IP infringement indemnity usually requires the customer to comply with the same kinds of procedural obligations – prompt notice of an IP infringement claim, conduct and control of defence and settlement of an IP infringement claim and cooperation regarding an IP infringement claim – that apply to a general indemnity.

## Additional Remedies

SaaS agreements usually require the service provider to provide the customer with additional remedies if an IP infringement claim affects the customer's continuing use of the SaaS. Those remedies typically include some or all of the following: (1) the service provider will obtain rights for the customer to continue to use the SaaS without a risk of the IP infringement claim; (2) the service provider will modify the SaaS so that the SaaS is no longer infringing but provides the same benefit to the customer; or (3) the service provider will terminate the customer's SaaS subscription and refund the unused portion of pre-paid fees for the terminated subscription, in which case the customer must stop using the SaaS.

## Exclusive Remedies

SaaS agreements often provide that an IP infringement indemnity and additional remedies are the customer's only remedies against the service provider if a third party makes an IP infringement claim against the customer. This exclusivity means that if an IP infringement claim prevents the customer from using the SaaS or causes the customer to suffer loss, damage or liability that is not covered by the IP infringement indemnity, then the customer might not be entitled to compensation from the service provider.

## Recommendations

When negotiating a SaaS agreement, the customer should understand the limited protections provided by the IP infringement indemnity and the potential risks (e.g., early termination) presented by the additional remedies. Customers should consider procuring insurance for residual risk. ■

# Confidentiality Obligations

SaaS agreements often impose restrictions and requirements regarding each party's use and disclosure of the other party's confidential information. The customer should ensure that the confidentiality obligations are sufficient, reasonable and practicable.

## Confidentiality Restrictions/Requirements

Confidentiality provisions impose restrictions and requirements on a party (the "Receiving Party") regarding the use and disclosure of the confidential information of the other party (the "Disclosing Party"). Those obligations can be adjusted to reflect the nature of the Disclosing Party's confidential information, the purposes for which the Receiving Party may access and use the information and the potential risks to the Disclosing Party if the information is misused. For example:

- Definition of "Confidential Information": The information to be treated as confidential might be defined broadly (e.g., all non-public information disclosed or made available by the Disclosing Party) or narrowly (e.g., information that is expressly identified in writing as confidential).
- Exceptions: The confidentiality obligations might not apply to certain kinds of information (e.g., information already known to the Receiving Party or subsequently obtained by the Receiving Party from another source that is not subject to confidentiality obligations).
- Permitted Use: The purposes for which the Receiving Party may use confidential information might be narrow (e.g., only the specific purpose for which the information was disclosed) or broad (e.g., as reasonably required to perform obligations and exercise rights under the SaaS agreement).
- Permitted Users: There might be restrictions on the individuals who may access and use confidential information (e.g., only the Receiving Party's employees on a need-to-know basis).
- Restricted/Permitted Disclosures: There might be express or implied restrictions on the Receiving Party's disclosure of confidential information to subcontractors, service providers and advisors. There might be procedural requirements for compliance with mandatory disclosures required by law (e.g., prior notice to and cooperation with the Disclosing Party).
- Protection/Standard of Care: The Receiving Party's obligation to protect confidential information might be absolute or limited to a specific standard of care (e.g., the same measures the Receiving Party uses to protect the Receiving Party's own confidential information, but not less than reasonable care).
- Duration: The confidentiality obligations might last for a specified period (e.g., five years after the end of the SaaS agreement) or until an item of information is no longer confidential.

## Return/Destruction Obligation

Confidentiality provisions usually require the Receiving Party to return to the Disclosing Party or permanently delete and destroy all records of confidential information in the Receiving Party's possession or control when the Receiving Party no longer has a legitimate need to use or retain the records or when requested to do so by the Disclosing Party. However, there are often exceptions that permit the Receiving Party to retain specified records of confidential information (e.g., secure electronic archives) or records of confidential information required for legal compliance or contract administration/enforcement purposes.

Confidentiality provisions often require the Receiving Party to confirm in writing that it has complied with its obligation to delete and destroy confidential information.

## Liability/Enforcement

The parties' liability for breach of confidentiality obligations is often an exception to provisions that exclude or limit the parties' liability for breach of the SaaS agreement. In those circumstances, the Receiving Party faces a risk of unlimited liability for all damage and loss suffered by the Disclosing Party as a result of the Receiving Party's breach of confidentiality obligations.

Confidentiality provisions often give the Disclosing Party special enforcement remedies, including a right to inspect and verify the Receiving Party's compliance with the confidentiality obligations, and confirm the Disclosing Party's right to judicial remedies (e.g., an injunction) to prevent the Receiving Party from breaching the confidentiality obligations.

## Administrative Practices

Confidentiality provisions might require the Receiving Party to implement administrative practices (e.g., internal policies and procedures) for handling the Disclosing Party's confidential information. In some circumstances, required administrative practices can be a significant burden and impose potentially substantial costs on the Receiving Party.

## Customer Data/Information

In addition to confidentiality provisions, SaaS agreements usually contain provisions regarding the security, confidentiality, integrity and availability of the data/information that will be processed and stored by or on behalf of the customer using the SaaS. Those provisions should be consistent and drafted to avoid uncertainty about the parties' rights, obligations and liabilities.

## Recommendations

When negotiating a SaaS agreement, the customer should ensure that the confidentiality obligations in the agreement are sufficient, reasonable and practicable in the circumstances (including the kinds of information that each party will disclose to the other party and the manner in which each party will use the other party's information). The customer should also carefully consider the customer's ability to establish and implement administrative practices required to comply with confidentiality obligations regarding the service provider's confidential information. ■

# Remedy Restrictions/Liability Limitations and Exclusions

SaaS agreements usually contain provisions that limit the customer's rights and remedies against the service provider for damage, loss or liabilities caused by the service provider's breach of the agreement or other misconduct. The customer should understand the risk allocation resulting from those provisions, and manage and mitigate risk through prudent business practices and insurance.

## Remedy Restrictions

SaaS agreements usually restrict the customer's remedies against the service provider if the SaaS or ancillary services fail to comply with contractual requirements. For example, the customer's remedies for a deficient SaaS might be limited to correction of the SaaS and limited financial credits against future subscription fees. The customer might also be entitled to limited financial credits against future fees if ancillary services fail to meet contractual requirements. If the specified remedies are exclusive, then the customer might not be able to terminate the SaaS subscription (unless expressly permitted by the SaaS agreement) or obtain from the service provider any compensation for damage, loss or liabilities caused by the deficient SaaS or ancillary services.

## Liability Limitations and Exclusions

SaaS agreements usually contain provisions – known as "liability limitations" – that limit or cap the amount of the service provider's potential liability to the customer for damage, loss and liabilities caused by the service provider's breach of contract or other misconduct. Liability limitations often impose a cap that is a specified amount or is determined by a formula based on the fees paid by the customer.

SaaS agreements also usually contain provisions – known as "liability exclusions" – that limit the service provider's potential liability to "direct damages", and exclude liability on the part of the service provider for all other kinds of damages (e.g., indirect damages, consequential damages, special damages and punitive damages) and specific losses (e.g., loss of business, loss of revenue, loss of profit, loss of data and loss of customer goodwill) suffered by the customer regardless of the cause. Liability exclusions often prevent the customer from recovering from the service provider financial compensation for the kinds of damage and loss that are most likely to result from a deficient SaaS or ancillary services or wrongful conduct by the service provider.

Liability limitations and exclusions are often subject to exceptions for specific kinds of damage and loss (e.g., bodily injury or physical damage to tangible property), for damage and loss caused by breach of specified contractual obligations (e.g., confidentiality and data protection obligations) or specified kinds of misconduct (e.g., infringement of intellectual property rights), or for certain financial obligations (e.g., indemnity obligations). The exceptions can significantly reduce the protection that the liability exclusions and limitations provide to the service provider and the customer.

## Recommendations

When negotiating a SaaS agreement, the customer should understand the risk allocation resulting from contractual remedy restrictions, liability limitations and liability exclusions, and should manage and mitigate risk through prudent business practices (e.g., business continuity plans, data backups and risk allocation provisions in contracts with potential third-party claimants) and insurance for residual risk. ■

# Term, Suspension and Termination

SaaS subscriptions and ancillary services are usually time-limited and subject to suspension or early termination in specified circumstances. The customer should understand the term of each SaaS subscription and ancillary services and take reasonable precautions to properly exercise renewal rights and avoid suspension or unintended early termination.

## Term

A SaaS agreement usually specifies the "term" or duration of the SaaS subscription and the service provider's ancillary services (e.g., technical support and problem resolution).

A SaaS subscription usually expires when the specified subscription term ends, but the SaaS agreement might provide for the renewal or extension of the subscription term. A renewal or extension might be automatic (unless a party opts out), at the customer's sole option, or require the agreement of both the service provider and the customer. Optional renewals and extensions are usually subject to pre-conditions, such as timely renewal notice and prompt payment of fees. Optional renewals and extensions that can be invoked by the customer provide certainty (e.g., specified fees) but usually afford limited flexibility. Renewals that require the agreement of both the service provider and the customer provide flexibility but no certainty.

Fees payable for a SaaS subscription and ancillary services often reflect the length of the subscription term and the customer's ability to renew or extend the subscription term. Fees payable for automatic or optional subscription term renewals or extensions are usually predetermined or based on a formula that permits reasonable fee increases.

## Suspension

SaaS agreements often permit the service provider to suspend the customer's use of the SaaS and ancillary services if the customer breaches specified obligations under the agreement (e.g., the customer fails to make a required fee payment) or in other specified circumstances (e.g., to prevent or remedy a security breach). A service provider's suspension rights are often subject to procedural requirements (e.g., notice to the customer and a reasonable opportunity for the customer to remedy the breach). A service provider is usually required to reinstate suspended services when the reasons for the suspension have been resolved.

## Termination

SaaS agreements usually allow the service provider and the customer to terminate the SaaS agreement as a whole (i.e., all SaaS subscriptions and ancillary services) or only specific SaaS subscriptions and services.

SaaS agreements usually contain different kinds of termination provisions. For example, termination for convenience (which allows a party in its discretion to terminate for the party's sole convenience), termination for breach (which allows a party to terminate if the other party breaches the agreement or specified provisions in the agreement), and termination in other specified circumstances (e.g., if the other party becomes insolvent or bankrupt). Termination provisions often include procedural requirements (e.g., a notice to the breaching party and a reasonable opportunity for the breaching party to remedy the breach) and restrictions (e.g., exercise of termination rights within a specified period) designed to prevent unreasonable termination.

The service provider and the customer might also have implied termination rights under generally applicable law. The nature and extent of implied termination rights will depend on the particular circumstances and the provisions of the SaaS agreement.

## Recommendations

When negotiating a SaaS agreement, the customer should understand the term of the SaaS subscription and ancillary services (including the customer's renewal and extension rights) and the circumstances in which the SaaS subscription and ancillary services may be suspended or terminated by the service provider or the customer. The customer should take reasonable precautions to properly exercise renewal or extension rights and avoid circumstances that present a risk of suspension or early termination by the service provider, particularly if the SaaS is essential for the customer's daily business operations. ■

# Consequences of Expiration/Termination and Surviving Rights and Obligations

SaaS agreements often specify important rights and obligations that are triggered when the SaaS subscription ends, or that continue to apply after the SaaS agreement ends. Those rights and obligations often vary depending on whether the SaaS agreement expires at the end of its prescribed term or is terminated early. The customer should understand those rights and obligations, and be prepared to enforce and comply with them.

## Consequences of Expiration/Termination

SaaS agreements usually require the customer to stop using the SaaS, and delete or destroy all copies of related documentation, when the SaaS subscription ends, and often require the customer to certify in writing that the customer has complied with those obligations.

If a SaaS is essential for the customer's daily business operations or difficult and time-consuming to replace, then the SaaS agreement might give the customer an optional transition period during which the customer may continue using the SaaS while the customer transitions to replacement software or services. The customer's right to invoke an optional transition period might be subject to restrictions (e.g., on expiration but not early termination of the SaaS subscription) and requirements (e.g., timely notice and advance payment of applicable fees).

SaaS agreements usually permit the customer to retrieve all of the customer's data from the SaaS during a limited period after the SaaS subscription ends, and require the service provider to securely delete all of the customer's data after the end of the data-retrieval period.

SaaS agreements might also specify other consequences of early termination of a SaaS subscription, such as a refund of pre-paid fees (if the customer terminates the SaaS subscription because of the service provider's breach) or accelerated payment obligations (if the service provider terminates the SaaS subscription because of the customer's breach).

## Surviving Rights and Obligations

SaaS agreements usually identify provisions that continue to apply, for a limited period or indefinitely, after the agreement ends. For example, provisions regarding intellectual property, data (including personal information) and confidential information, liability limitations and exclusions, indemnity obligations and dispute resolution procedures. Surviving provisions can impose substantial burdens and potentially significant risks and liabilities on the service provider and the customer.

## Recommendations

When negotiating a SaaS agreement, the customer should ensure that the customer's rights and obligations that are triggered when the SaaS subscription ends, or continue after the SaaS agreement ends, are consistent with the customer's business requirements and legal obligations. The customer should be prepared to enforce and comply with those rights and obligations. ■

# Governing Law and Dispute Resolution

SaaS agreements usually specify the law that governs the agreement and a procedure and venue for resolving disputes relating to the agreement. The customer should ensure that the governing law is appropriate and the dispute resolution procedure and venue are suitable and fair to both the service provider and the customer.

## Governing Law

To properly negotiate a SaaS agreement and to perform obligations and exercise rights under the agreement, the service provider and the customer must understand the legal rules that govern the interpretation and enforcement of the agreement. Those legal rules will be determined primarily by the law of a particular jurisdiction, which is commonly known as the "governing law". The governing law is important because different jurisdictions have different legal rules relevant to SaaS agreements, and even a small difference in legal rules can have a significant effect on the rights and obligations of the service provider and the customer.

Under Canadian law, a SaaS agreement is usually governed by the law specified in the agreement or, if the governing law is not specified, the law of the jurisdiction that has the most real and substantial connection to the agreement. If there is a dispute regarding a SaaS agreement that does not specify the governing law and has connections to multiple jurisdictions (e.g., the service provider and the customer are in different countries), then a court or arbitrator will determine the governing law by identifying the jurisdiction that has the most real and substantial connection to the agreement.

It is usually best if a SaaS agreement specifies the governing law, so that the service provider and the customer know with certainty the law that governs the interpretation and enforcement of the agreement. Most parties prefer their local law to be the governing law, but a different law might be better. The service provider and the customer should select a governing law based on careful consideration of the law's potential effect on all aspects of the interpretation and enforcement of the agreement.

The selection of a governing law presents considerations of cost and risk. A party that is not familiar with a proposed foreign governing law must either obtain legal advice from a lawyer qualified to provide advice regarding the governing law or accept the risk that the governing law is materially different from the law of the party's jurisdiction.

## Dispute Resolution

SaaS agreements usually specify a procedure for resolving disputes between the service provider and the customer, and often confirm that the service provider and the customer will continue to perform their respective obligations under the agreement during the resolution of disputes. If a SaaS agreement does not specify a dispute resolution procedure, then all disputes relating to the SaaS agreement will be resolved through conventional litigation unless the service provider and the customer agree to resolve a dispute using an alternative dispute resolution procedure.

There are four basic dispute resolution procedures:

- Negotiation – one or more rounds of direct confidential negotiation by representatives of the service provider and the customer, with each round involving more senior representatives.
- Mediation – confidential negotiation facilitated by an independent and neutral individual (known as a "mediator") who assists the service provider and the customer to negotiate a settlement of the dispute, but does not have authority to make binding decisions or impose a binding resolution.
- Arbitration – adjudication through a private and confidential adversarial process in which the service provider and the customer present evidence and argument to one or more independent decision-makers (known as "arbitrators") who have authority to make binding decisions and impose a binding resolution that is subject to review by a court in limited circumstances.
- Litigation – adjudication through a public adversarial process in the applicable court system in which the service provider and the customer present evidence and argument to a judge who has authority to make binding decisions and impose a binding resolution that is subject to review by an appellate court.

Each dispute resolution procedure has comparative advantages and disadvantages, including varying degrees of privacy/confidentiality, speed and finality. The optimal dispute resolution procedure will depend on the nature and circumstances of the SaaS transaction and the preferences of the service provider and the customer.

The location (also known as "venue") of dispute resolution proceedings does not have to be in the governing law jurisdiction. The dispute resolution venue can impose significant costs and logistical burdens on either or both the service provider and the customer. Dispute resolution proceedings in a party's local venue can be much more convenient than proceedings in a foreign venue. If the service provider and the customer are in different jurisdictions, then they might negotiate a compromise by selecting a neutral dispute resolution venue or agreeing that the party commencing dispute resolution proceedings will do so in the other party's preferred venue.

## Recommendations

When negotiating a SaaS agreement, the customer should: (1) understand the legal rules that govern the interpretation and enforcement of the agreement; (2) ensure that the dispute resolution procedure is reasonable and appropriate in the circumstances; and (3) ensure that the dispute resolution venue is reasonable and fair based on the relative convenience/inconvenience of the venue to both the service provider and the customer. ■

# Boilerplate Provisions

SaaS agreements usually contain numerous provisions – known as "boilerplate" provisions – that deal with various miscellaneous matters. Boilerplate provisions can have a significant effect on the interpretation of the SaaS agreement and the rights and obligations of the service provider and the customer.

## Publicity

SaaS agreements often include a provision that allows the service provider to publicize the customer's use of the SaaS and use the customer's branding for those purposes. If that kind of publicity is not acceptable to the customer, or if the customer requires control over the use of the customer's branding, then the customer should negotiate a revision to the publicity provision to require the service provider to obtain the customer's prior written approval of the service provider's use of the customer's name and branding.

## Notices

SaaS agreements usually include a provision that requires all notices under the agreement be given in writing and delivered by specified methods to designated addresses. The customer should ensure that the specified delivery methods are appropriate for the kinds of important notices (e.g., notices regarding subscription renewal or extension, breach, termination, and dispute resolution) that might be given by the customer and the service provider under the agreement. The customer should strictly comply with the notice requirements when giving a notice to the service provider.

## Waivers/Consents

SaaS agreements usually include a provision that purports to render ineffective any consent by a party to the other party's non-compliance with the agreement, or any waiver by a party of its rights under the agreement, unless the consent or waiver is confirmed in writing and signed by the consenting or waiving party. Consequently, the customer should obtain the service provider's signed written confirmation of each consent or waiver.

## Amendments and Changes

SaaS agreements usually include a provision that purports to render ineffective any amendment to the agreement that is not confirmed in writing and signed by both the service provider and the customer. Consequently, the customer should ensure that all amendments to the SaaS agreement, including promises by the service provider made after the agreement is signed, are confirmed in a written and signed document.

Some SaaS agreements permit the service provider to unilaterally change important ancillary documents that are incorporated by reference into the agreement (e.g., documents that specify details of the SaaS or ancillary services). The customer should ensure that any unilateral changes by the service provider are subject to reasonable restrictions (e.g., no changes that diminish the availability or quality of the SaaS or ancillary services) and requirements (e.g., prior notice of all changes).

## Assignment

SaaS agreements usually include a provision that prohibits the customer from assigning the agreement without the service provider's prior consent. That restriction might present significant difficulties for the customer if the SaaS is costly, difficult to replace or essential to the customer's daily business operations. In those circumstances, the customer might require a revision to the assignment provision to permit the customer to assign the agreement without the service provider's consent in limited circumstances (e.g., in connection with the customer's participation in a corporate merger, acquisition or internal restructuring or a sale of all or substantially all of the customer's business and assets) and subject to reasonable requirements (e.g., the assignee agrees in writing to be bound by the SaaS agreement).

## Rules of Interpretation

SaaS agreements usually include a provision that specifies rules for the interpretation of the agreement. For example, headings are for reference only, "days" means calendar days, and "including" means including without limitation or restriction. Those rules of interpretation are important because they can affect the meaning and effect of the SaaS agreement.

## Recommendations

When negotiating a SaaS agreement, the customer should be mindful of the boilerplate provisions that affect the meaning and effect of the agreement and the customer's rights and obligations under the agreement. The customer should consider whether the boilerplate provisions require revision to be appropriate in the circumstances. ■

# Contract Interpretation Principles

When negotiating a SaaS agreement, the customer should understand the basic legal principles that will govern the interpretation of the agreement in the event of a dispute. In most circumstances, the customer's rights and obligations will be defined and limited by the express words of the agreement (including external documents incorporated by reference into the agreement), which will be given their ordinary and natural meaning.

## Interpretation Rules

A court will interpret a SaaS agreement by following generally applicable contract interpretation rules. A court will read a SaaS agreement as a whole, giving the words in the agreement their ordinary and grammatical meaning consistent with the surrounding circumstances known to the parties at the time the agreement is made. The meaning of the words in a SaaS agreement may be derived from contextual factors (e.g., the purpose of the agreement and the nature of the relationship created by the agreement), but a court will not rely on the surrounding circumstances to overwhelm the words in the agreement and effectively make a new agreement for the parties. In addition, a court will not consider evidence of the parties' subjective intention or understanding regarding the meaning or effect of a SaaS agreement.

## External Contract Documents

Some SaaS agreements are presented as a relatively short and simple document that incorporates by reference other documents (e.g., standard form terms and conditions, service level agreements and data processing addenda) that are available to the customer (e.g., on the service provider's website) when the agreement is signed by the customer but are not physically attached to the agreement. In most cases, those external contract documents, which often deal with important business, technical and legal issues, will be part of the SaaS agreement even if the customer does not access or read the documents.

## Signatures and Acceptance

In most circumstances, a signature (including an electronic signature) on a contract document or the electronic acceptance of a contract document (e.g., by clicking an "I Agree" or similar online button) is a binding confirmation that the signer accepts and agrees to the contract. A person who signs or electronically accepts a contract will usually not be permitted to later reject the contract on the basis that the person did not read or understand the contract (including external documents incorporated by reference into the contract) or intend to be bound by the contract. Consequently, in most cases, a customer will be bound by a SaaS agreement signed or electronically accepted by or on behalf of the customer regardless of the customer's actual, subjective understanding or intention.

## Recommendations

When negotiating a SaaS agreement, the customer should carefully review the entire SaaS agreement (including external documents incorporated by reference) to ensure that the agreement as a whole, when given its ordinary and grammatical meaning, accurately and completely sets out the intended agreement regarding the SaaS and all related matters. ■

# Key Questions for SaaS Agreement Negotiation

Following are some key questions that a customer should consider when negotiating a SaaS agreement.

## Procurement Process

- Has the customer conducted appropriate due diligence of the SaaS service provider and the SaaS?
- Has the customer assessed the relative benefits and risks of the intended use of the SaaS, and considered potential risk mitigation measures?

## SaaS Subscription

- Does the SaaS subscription properly identify all modules, features and functionalities of the SaaS?
- Does the duration and scope of the SaaS subscription allow the customer and other relevant persons (e.g., corporate affiliates and subsidiaries) to use the SaaS as required for current and reasonably anticipated future needs?
- Does the customer have the right to periodically change the scope of the SaaS subscription?
- If the SaaS agreement requires the customer to periodically report the customer's use of the SaaS, then are those reporting obligations reasonable and practicable?
- If the SaaS agreement gives the service provider audit rights, then are those audit rights reasonable and practicable?
- Can the customer implement reasonable measures to prevent use of the SaaS and documentation in breach of the SaaS agreement?

## Warranties and Remedies

- Does the SaaS agreement contain appropriate promises by the service provider regarding the availability and quality of the SaaS, and specify sufficient and reasonable remedies if the SaaS is deficient?
- Does the SaaS agreement accurately confirm all of the commitments made by the service provider during sales presentations and negotiations, and provide the customer with reasonable and appropriate rights and remedies if the service provider breaches those commitments?

## Acceptance Testing

- If the customer requires an opportunity to conduct acceptance testing of the SaaS, then does the SaaS agreement: (1) permit the customer to conduct reasonable acceptance testing of the SaaS; (2) specify appropriate acceptance criteria; and (3) provide the customer with reasonable remedies if the SaaS fails acceptance testing?

## Ancillary Services (Technical Support and Problem Resolution)

- Does the SaaS agreement contain appropriate commitments by the service provider regarding ancillary services, including technical support and problem resolution?
- Does the SaaS agreement contain promises by the service provider regarding the quality of ancillary services and provide the customer with reasonable remedies if the ancillary services are deficient?

## Fees

- Does the SaaS agreement specify the fees payable for the SaaS and ancillary services throughout the expected duration of the SaaS subscription?
- Does the SaaS agreement specify the fees for changes to the scope of the SaaS subscription (e.g., additional usage rights) and ancillary services?
- Does the SaaS agreement provide the customer with reasonable protection against future fee increases for additional usage rights and ancillary services?
- Does the SaaS agreement allow the customer a reasonable opportunity to cure any inadvertent breaches of payment obligations before the service provider suspends or terminates the subscription?

## Customer Data and Information

- Does the SaaS agreement include provisions regarding the data/information that will be processed and stored in the SaaS that are reasonable and sufficient for compliance with all applicable laws (including personal information protection laws), the customer's obligations and duties to third parties, and recommended best practices?
- Is the customer able to manage and mitigate data/information risks through prudent business practices?

## Indemnities

- Does the SaaS agreement contain reasonable and appropriate general indemnities against relevant third-party claims?
- Does the SaaS agreement contain a reasonable and appropriate intellectual property infringement indemnity and sufficient additional remedies for intellectual property infringement claims?
- Is the customer able to establish and implement practices to manage and mitigate risks of third-party claims and liabilities, and obtain insurance for residual risk?

## Confidentiality

- Does the SaaS agreement contain confidentiality provisions that are sufficient, reasonable and practicable?
- Is the customer able to establish and implement administrative practices required to comply with confidentiality obligations regarding the service provider's confidential information?

## Remedy Restrictions

- If the SaaS agreement imposes restrictions on the customer's remedies for deficient SaaS or services, then are those restrictions reasonable in the circumstances?

## Liability Limitations/Exclusions

- If the SaaS agreement imposes limits on the liability of the service provider or the customer, then are the limits reasonable and subject to appropriate exceptions?
- If the SaaS agreement excludes liability on the part of the service provider or the customer for certain kinds of damage and loss, then are the exclusions reasonable and subject to appropriate exceptions?
- Is the customer able to establish and implement practices to manage and mitigate risks of damage and loss, and obtain insurance for residual risk?

## Term and Termination

- Is the duration (term) of the SaaS sufficient?
- In what circumstances can the SaaS subscription be extended or renewed by the customer, and is there certainty regarding fees payable during the extension or renewal period?
- In what circumstances can the SaaS subscription or the entire SaaS agreement be suspended or terminated by the service provider or the customer, and is suspension or termination subject to appropriate restrictions and procedural requirements?

## Consequences of Expiration/Termination

- What are the consequences of the expiration or termination of the SaaS subscription or the entire SaaS agreement?
- What rights and obligations are triggered when the SaaS subscription ends or continue after the SaaS agreement ends, and do those rights and obligations satisfy the customer's business requirements and legal obligations?

## Governing Law and Disputes

- What law governs the SaaS agreement, and how does the governing law affect the interpretation and enforcement of the agreement and the rights and obligations of the service provider and the customer?
- Does the SaaS agreement specify an appropriate procedure for resolving disputes relating to the SaaS agreement?
- Does the SaaS agreement specify a venue for resolving disputes relating to the SaaS agreement, and is the venue reasonable and fair to both the customer and the service provider?

## Miscellaneous

- Are the service provider's publicity rights acceptable?
- Is the procedure for giving contractual notices appropriate?
- Can the customer assign the SaaS agreement without the service provider's consent in appropriate circumstances? ■

# Glossary

**Acceptance criteria:** The requirements for the availability, functionality, performance, operation and results of a SaaS.

**Acceptance testing:** A procedure for the customer to review and test a SaaS to determine whether the SaaS conforms to the applicable acceptance criteria.

**Credentials:** Unique identifiers (e.g., user names, passwords and other factors) required to access and use a SaaS, which are used by the service provider to help enforce certain kinds of SaaS subscription restrictions and requirements and prevent unauthorized use of a SaaS.

**Disclaimer:** A contract provision that excludes specified promises or obligations, including promises or obligations that might otherwise be implied by law.

**Entire agreement clause:** A contract provision that confirms that the contract supersedes and replaces all prior discussions, promises, understandings and agreements between the parties regarding the subject matter of the contract.

**Indemnity:** A contractual obligation that requires a person (known as the "indemnitor") to protect another person (known as the "indemnitee") against specified claims against the indemnitee, specified damages and losses suffered by the indemnitee or specified liabilities incurred by the indemnitee.

**IP infringement indemnity:** An indemnity that protects the indemnitee against claims that the indemnitee has infringed third-party intellectual property rights.

**Liability exclusion:** A qualitative restriction on the kinds of damages for which a person may be liable.

**Liability limitation:** A quantitative limit or cap on the amount of a person's liability.

**License:** A legal permission given by a person (known as the "licensor") to another person (known as the "licensee") to do something that would otherwise be an infringement of the licensor's legal rights.

**Problem resolution:** A service that provides technical assistance to resolve problems with a SaaS.

**Representation:** A promise about a present fact.

**Service Level Agreement or SLA:** An agreement, or part of an agreement, that sets out a service provider's promises about the level or quality of specific services.

**Software-as-a-Service or SaaS:** An internet-based service that makes computer software and related information technology infrastructure available as a utility or consumption-based service.

**Subscription:** A license to use a product or service (e.g., a SaaS) for a specified period.

**Technical support:** A service that provides technical advice regarding the use of a SaaS.

**Warranty:** A promise about a future fact.

Calgary
Centennial Place, East Tower
520 3rd Ave S W, Suite 1900
Calgary, AB, Canada  T2P 0R3
T  403.232.9500  |  F  403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada  H3B 5H4
T  514.879.1212  |  F  514.954.1905

Ottawa
World Exchange Plaza
100 Queen St, Suite 1300
Ottawa, ON, Canada  K1P 1J9
T  613.237.5160  |  F  613.230.8842 (Legal)
F  613.787.3558 (IP)  |  ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400
Toronto, ON, Canada  M5H 4E3
T  416.367.6000  |  F  416.367.6749

Vancouver
1200 Waterfront Centre
200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada  V7X 1T2
T  604.687.5744  |  F  604.687.1415

Canada's Law Firm



Borden Ladner Gervais