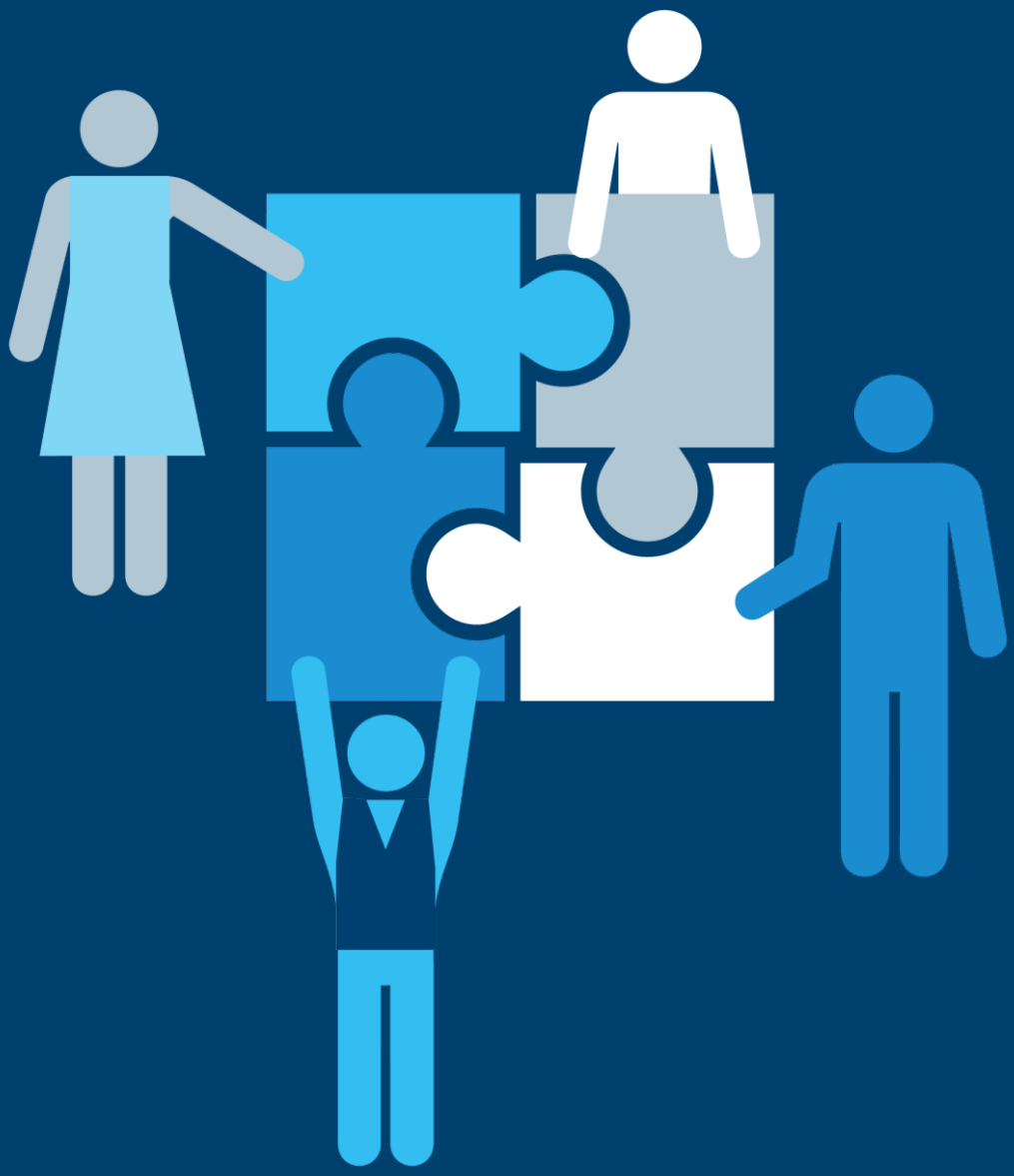
SaaS Contracting Guide



June 2023

World Commerce & Contracting

SaaS Contracting Guide

This SaaS Contracting Guide provides guidance in dealing with SaaS contracts and assumes the reader has a basic knowledge of contract terms and cloud but wants to learn more about the unique contractual issues specific to SaaS relationships. It covers the key areas of SaaS contracts and addresses how the World Commerce & Contracting (World CC) Contracting Principles apply (and don't apply) to SaaS contracts due to the operational realities of SaaS.

This guide addresses the common terms for public cloud SaaS solutions (as opposed to private cloud SaaS or SaaS-related professional services) and has been written so that it can be relied upon by both buyers and sellers of SaaS services for a fair and balanced contract. Variations may be needed depending on the technical and business specifics of the SaaS offering, the willingness and ability of the vendor to cater to the needs of individual customers, and local contracting practices and laws.

This SaaS Contracting Guide is made up of four sections:

I. Overview of SaaS
II. Summary of Key Contracting Issues for SaaS
III. SaaS Contract Checklist
IV. Applicability of the World CC Contracting Principles to SaaS

This document does not provide legal advice or counsel.

World CC recognizes and thanks the following people who contributed to the development of this document:
Laurie Ehrlich, Chief Commercial Counsel, Datadog, Inc.
Hal Bretan, Contracting Standards Executive in Residence, World Commerce & Contracting
Vincent Denoyelle and Killian Lefevre from the law firm of Eversheds Sutherland

I. Overview of SaaS

What is SaaS?
Software as a Service is a cloud-based software service delivery model. This means that it is:

- **Subscription-Based:** SaaS is offered most frequently based on flat subscription pricing (e.g., monthly, quarterly, annually) or, in some cases, based on pay-as-you-go basis (e.g., based on number of users, volumes of usage). Subscriptions are commitments by both parties to maintain the relationship through the full term of the applicable order and typically can either not be terminated for convenience mid-term or can be terminated early without cause only upon payment of a termination charge.

- **Multi-Tenant:** Most SaaS offerings are multi-tenant, which means that a single instance of the software and infrastructure serves multiple customers. While each customer's data is isolated and remains invisible to other customers, the infrastructure (including the security controls) and services are the same for all customers and cannot be customized on an individual customer-by-customer basis (except with respect to the standard customization options that are part of the SaaS design).

- **Web-based and (usually) Third-Party Cloud Hosted:** All SaaS is web-based rather than installed on local computers or on-premises servers. This means that updates and maintenance are controlled by the SaaS vendor. Most SaaS offerings are hosted on third-party cloud service providers ("CSPs") such as AWS, GCP and Azure so vendors can provide high-availability, enterprise-grade services to their customers.

- **Agile and elastic:** SaaS is not static, and it can be upgraded continuously and so can associated features, security settings and service levels. SaaS is elastic and typically will be regularly adapted by the SaaS vendor to meet market demand and needs as well as changes in technology and security risks. When the SaaS changes, the documentation is updated as needed to match the changes.

- **Shared-responsibility model:** As is the case for all cloud-based contracts, SaaS is based on a shared responsibility model whereby the customer is responsible for access to the SaaS platform and the data input to the SaaS platform, and the vendor is responsible for the platform itself (application, OS, etc.).

II. Summary of Key SaaS Contracting Issues

Key Issues for SaaS
A. The customer will be able to use the SaaS solution and the vendor will provide access to the SaaS solution. B. The customer has reasonable assurances of quality, and the vendor can continue to develop and deploy the SaaS solution without unreasonable customer impediments. C. Pricing and schedule for payments are clear. D. There are appropriate mechanisms to safeguard the SaaS solution and the customer data. E. There are no unexpected transfers of ownership. F. Risk apportionment is balanced. G. Termination rights are clear.

How SaaS is different from Software		How SaaS is different from Professional Services	
SaaS fact:	***SaaS fact means:***	***SaaS fact:***	***SaaS fact means:***
SaaS enables constant development and improvement of the software without any customer effort (although customers can impact the evolution of the software by reporting bugs or requesting new features).	In SaaS, there is generally no right to stay on "older" software versions for any extended length of time.	SaaS vendors provide and support the services 24/7 without the customer separately paying per hour for those employees or paying for particular projects associated with the software.	In SaaS, there are no vendor employees dedicated to providing services to a single customer.
SaaS means all infrastructure including hosting and data storage is the responsibility of the SaaS vendor and is the same for all customers linked to that infrastructure.	In SaaS, there is no option to design the SaaS infrastructure to meet bespoke requirements.	SaaS is deployed and offered as described in the documentation and does not include unique deliverables.	In SaaS, negotiated project specifications, testing, and launch are not part of the service.
All SaaS customers have the same product options available to them.	In SaaS, there is no bespoke customer design option except for the already built-in customer configuration options.	SaaS architecture generally relies on products provided by other vendors and SaaS vendors need flexibility to change those vendors at will without a veto by individual customers.	In SaaS, customer cannot approve or reject any specific personnel used to provide the SaaS.

III. SaaS Contract Checklist

This checklist focuses on the key issues for SaaS identified in Section II, above, and provides explanatory notes on what you should expect (or not expect to see) in a SaaS contract. This checklist is not a complete list of the terms you would expect to see in a SaaS contract, but those that are unique to SaaS or shaped by SaaS. For other clauses that are consistent with SaaS (as indicated in Section IV, below), you can find more information in the WorldCC Contracting Principles.

Issue	Concepts in SaaS Contracts	Concepts Typically Not in SaaS Contracts
A. The customer will be able to use the SaaS solution and the vendor will provide access to the SaaS solution.	❑ Access and Use ❑ Services definition ❑ Data portability post-termination ❑ Authorized Users ❑ Restrictions on use ❑ Suspension ❑ Review rights by the party who does not have access to the usage data	❑ Deliverables ❑ Transition assistance

Checklist	Notes
❑ There is a right to access the services (and all purchased features and functions) during the order term.	SaaS contracts do not typically include broad license grants and instead provide the right or license to access and use the services. Normally, that access is provided in the form of a subscription for a defined initial period with options for extensions. As the customer is not downloading, installing, copying, or modifying software and/or the documentation (which is also available online), on-premise software license grants are not necessary. In addition, there is no language around deliverables or specifications with respect to the SaaS; as discussed below, the SaaS is being delivered "As-Is".
❑ There is a customer right to access/export the customer's data during the term and for a limited period post expiration/termination.	Most SaaS products include the ingestion of the customer's data and the processing of that data for the customer. The right to access the services is synonymous with the customer being able to access its data in the services, no additional grant is needed for the customer during the term. However, there should be an explicit right for the customer to have the right after expiration/termination to either access the services solely for the purposes of viewing and/or retrieving that data (typically a month post-termination) or to receive an export of its data (usually in whatever format it was available for export during the term). The customer should review those options as part of the SaaS selection process. SaaS vendors do not typically provide transition assistance services as part of the SaaS; that is considered an ancillary professional service. Each SaaS offering is specific to the vendor and therefore cannot be directly transferred to a new SaaS vendor; the only possible transfer is the customer's data.
❑ The vendor has a right to process the data that the customer inputs into the services solely to provide the services and for any other additional agreed upon uses.	SaaS products' value is typically based on how they process ingested customer data, so the agreement should include an explicit right for the SaaS vendor to process the customer's data and to use it to provide and support the services. In addition, there may be a grant allowing the SaaS vendor to include the data in aggregated and/or anonymized customer data sets. For SaaS products that include insights on the data, those insights are sometimes

	derived from the aggregated data inputted by all its customers. With the rise of AI, it is likely that the market is going to push most vendors to provide insight offerings. Customers should expect that to receive insights, they will have to agree that their inputs will be included in aggregated (and anonymized) data sets. Vendors should include mechanisms that enable them to exclude from data from customers that decide to opt out from contributing to and receiving insights and customers should consider whether the aggregation and anonymization is sufficient to prevent the recognition of their confidential information. The key focus should be on protecting sensitive information that belongs to the customer during that process. Anonymizing data may or may not be sufficient to safeguard the customers or its clients as, in some cases, parties who see that information can decipher where it came from. In those cases, the customer should be able to opt out or the agreement should have adequate protections for that data in the context of the vendor sharing that information with third parties. In addition to the input and output data, the agreement may cover the concepts of account data (user and billing information) and usage data (the data on how the services are being used). Usually, account data is governed by the privacy policy, and the vendor is considered a data controller of that data (as defined in the GDPR), and usage data is owned by the vendor (much the same as how a fast-food chain tracks how many burgers are purchased in any single store each hour).
❑ The definition of services in the agreement is broad enough to provide flexibility at the order level as to what products, features, and functions the customer is purchasing.	The parties should not need a new agreement or an amendment when the customer changes what they are purchasing (including obtaining new product offerings by the SaaS vendor). Orders should address the specific products included in the purchase, and change orders can be used to address additional purchases, such as additional users, locations, or features. The description of the services may include use descriptions, references to URLs, documentation, product names, and/or feature or function designations.
❑ There is a definition of authorized users that includes all of the customer's anticipated users.	The definition of authorized users should align with the pricing model. If pricing is user-based, the agreement or order should provide clarity around types and numbers of users. In addition, the definition of authorized users should include all anticipated customer users. This may include employees as well as employees of customer's affiliates, contractors/subcontractors, or sometimes customer's own clients, subject to any restrictions from the vendor. In all cases, the customer should be responsible for its users' compliance with any restrictions on the use of the services, including acceptable use policies ("AUPs"). If relevant to the SaaS product, the contract may also need to address the location of the users, but this will be solely at the country level to comply with licensing and import/export restrictions. There shouldn't be language around use only on certain computers or from certain offices, which are on-premise software license concepts.

❑ Use restrictions are reasonable.	In the agreement and/or an associated AUP, SaaS vendors include restrictions on use of the services that encompass illegal or harmful activities such as intellectual property ("IP") theft, copying, introduction of malicious code, behaviors that violate laws, and similar acts. Depending on the nature of the SaaS services there may also be country level restrictions necessary for compliance with the laws of certain jurisdictions. As all customer users will need to refrain from such activities, customers should make sure the listed prohibitions are limited to behaviors (i) that constitute acts that customer users would typically know are not permitted, and/or (ii) that customer knows that it will not engage in during its use of the services. The customer may want to provide training or advisories to each user to avoid prohibited conduct.
❑ Suspension rights apply at the account level only for non-payment, systemic breach, or temporary operational needs; otherwise they are limited to the individual users engaging in wrong-doing. Advance written notice should be required except in the case of imminent harm or risk to the platform. Customers should be given a reasonable opportunity to cure the cause of the suspension.	Given that SaaS is based on a right to access the service, the suspension mechanism is particularly relevant. A suspension could result from a breach of the agreement or AUP with or without notification depending on the type of breach. It could also be planned, for maintenance purposes, and would typically come with a reasonable prior notification mechanism. There will be cases where a suspension is necessary to protect the integrity or security of the SaaS platform and the data within it. In such cases, a prior notification requirement could delay the suspension and expose the SaaS platform and thus all customers to a risk of harm. Therefore, this situation would be an exception to the prior notice rule. This also reflects the fact that CSPs on which SaaS offerings rely, will have the same type of mechanism for emergency cases.

Issue	Concepts in SaaS Contracts	Concepts Typically Not in SaaS Contracts
B. The customer has reasonable assurances of quality and the vendor can continue to develop and deploy the SaaS solution without customer impediments.	❑ Warranty that service complies with documentation ❑ Disclaimers ❑ Availability in the form of SLAs ❑ Support ❑ Additional services ❑ Evaluation periods	❑ Deliverables ❑ Acceptance ❑ Change Control ❑ Upgrades and versioning ❑ Self-help as a remedy ❑ Customer control over subcontractors ❑ Source code escrow

Checklist	Notes
❑ There is a warranty that the services will perform in accordance with the documentation and that the documentation is accurate to the services.	The elastic nature of SaaS means that products are likely to change over the term of an order. The documentation should be updated along with the services, and this means that the documentation should be online (not attached to the agreement). To protect the customer, the agreement should have a warranty that the documentation and the services will be aligned throughout the term of the service. There may also be a warranty that the functionality of the services will not be materially diminished during the term. Note, the fact that SaaS is usually updated with a frequency exponentially higher than in an on-premise software model combined with the fact that SaaS includes not just the code, but also the infrastructure, the hosting, the inclusion of other vendor's services or content (as discussed below), means that source code escrow does not have a meaningful protective value and should not be included in the agreement.
❑ There are disclaimers aligned with the aspects outside of the vendor's control or where the customer is otherwise protected.	It is atypical for there to be other warranties and because the SaaS is not designed for any individual customer, it is standard for the SaaS to be provided "as is" with no promises (i) as to whether it will work with the customer's particular systems or meet customer expectations; (ii) that it will be error-free (problems can be identified by the customer and resolved through support tickets); and (iii) that it will not infringe any IP rights (here the customer is protected through the IP indemnity as described in Section F). Further, statutory or implied warranties are generally inapplicable and are therefore typically disclaimed.
❑ There is a commitment to having the services available for a minimum percentage of time each month (e.g., 98%, 99.9%).	One of the key differences between SaaS and on-premise software is that SaaS is not installed on individual computers; rather it is primarily accessed over the web. This means that the SaaS vendor, rather than the customer, is responsible for ensuring that the service is up and running for the duration of the term. The customer is usually protected from vendor failures in this area through a contractual commitment (SLA) to a minimum percentage of time each month that the service can be accessed, with exceptions for accessibility failures due to customer failures to use the services in accordance with the agreement or the documentation, force majeure, suspension of users, and maintenance windows. The availability commitment can be strengthened by including limits on the maintenance windows or by including credits for availability failures. The vendor's ability to make availability commitments, provide limited maintenance windows, and provide availability credits will depend on the SaaS maturity level and the pricing model. Remedies are limited to credits and/or termination for repeated or lengthy outages.
❑ There is an obligation to provide advanced notice	One of the big benefits of SaaS is how rapidly and frequently updates can be deployed. Some companies make little improvements almost daily and

of when the services will be inaccessible due to planned maintenance.	most make many changes over the course of any year. Generally, those updates do not interrupt customers' ability to use the services. When they are going to cause an interruption in the ability to access and use the services, notice should be provided in advance so that customer operations are not unexpectedly disrupted. Due to the short development and release timelines for updates in SaaS, it is unlikely that a SaaS vendor can provide notice more than seven days in advance for most maintenance disruptions (although they may be able to provide more advanced notice for certain planned material updates). As referred to above, additional controls can be put on the maintenance, such as total number of hours in a given month or specific windows for maintenance. However, because the multi-tenant environment means updates are released across many customers at the same time, custom controls such as mutually agreed timing, at times that don't disrupt the customer's business, during customer's non-business hours, or through a change control process are not options in SaaS.
❑ Basic support is included.	SaaS is typically designed to be user-friendly and self-help enabled through regularly updated documentation. Support may be needed at the outset of the service to answer operational or implementation questions and to ensure efficient adoption of the features of the software, and some SaaS companies offer this support or can recommend implementation specialists. Once the learning curve has passed, it is entirely possible to have full use of a SaaS product for years and never need any further assistance; however, for a long-term contract with high spend, it is good to ensure that assistance is available when needed. In addition to a general commitment to provide support, the contract may also have obligations around response times depending on the severity of the issue for which assistance is needed. In some cases, premium support services may be available for shorter response times or additional support channels. Note that commitments on resolution times (as opposed to response times) are normally not provided.
❑ Additional services may be included at the order or statement of work("SOW") level.	Some SaaS companies offer professional services around their SaaS products, such as enhanced technical support, start-up services, training, and consulting. Where these services are an optional additional purchase, the terms for these services should be at the order level or in a statement of work rather than at the subscription agreement level. It would be atypical for these professional services terms to include all of the terms you would see in a professional services agreement because SaaS-related professional services are usually provided by non-dedicated resources and generally are limited to the provision of materials, instructions, or practices that are universal for all of the SaaS vendor's customers rather than deliverables tied to customers' specifications or incorporating customer materials. Some professional services terms that are more likely to be relevant are performance warranties, timing, definitions of deliverables (if any). Work-for-hire IP transfer language should only be included if there are custom deliverables based on customer specifications that do not rely predominantly on the specifics of the SaaS itself.
❑ Use of subcontractors as part of the services is permitted, and the SaaS vendor is responsible for its subcontractors to the	At a minimum, SaaS vendors typically host their services with one or more CSPs and most make use of other vendors to deliver the full solution including other SaaS vendors for messaging, ticketing, and data analytics. As those uses are across all customers, SaaS vendors can't agree that any single customer can demand changes to, or specific requirements for, such vendors. An exception to this exists for

same extent it would be for itself.	subprocessors where data privacy regulations require the controller to be given an approval right. This is generally resolved in a data processing agreement ("DPA") through the provision of a time-bound objection right for the customer with respect to the use of any new subprocessor.
❑ There is an opportunity, before making a long-term commitment, to evaluate the vendor services.	Many SaaS vendors make it easy to sign up for a limited time trial of their services. Such trials are typically on the vendor's standard terms and free (unless the use of the services requires a significant upfront investment by the vendor or the customer wants an extended trial period, in which cases the evaluation may be a paid engagement). This evaluation period takes the place of the acceptance and testing procedures you would see in a contract for professional services or custom on-premise software. Unlike those contracts, in SaaS, there is no identification of specifications that the deliverables need to meet and no defined period for the customer to test the deliverables and accept or reject for reperformance.
❑	

Issue	Concepts in SaaS Contracts	Concepts Typically Not in SaaS Contracts
C. The pricing and payment schedule are clear.	❑ Subscription-based payment terms ❑ Overage fees if use exceeds pre-determined amount ❑ Auto-renewal ❑ Indirect purchases	❑ Implementation and set-up fees ❑ Maintenance fees ❑ Change control
Checklist	**Notes**	
❑ How the fees are calculated is clearly described.	In every contract, it is advisable to have clarity around pricing to avoid billing disputes down the line. While there is not one type of SaaS pricing, it is typically a subscription-based model - the customer subscribes to get access and the periodic recurring charges are based on the length and scope of the customer's commitment. SaaS pricing confusion typically arises around what SaaS solution components or ancillary offerings are included, how use relates to the calculation of fees, what happens when use is below (usually a committed amount is committed regardless of whether you use it) or above committed amounts (see section below), and when standard pricing may apply instead of negotiated pricing. These aspects should be clearly addressed in the agreement or the order. Maintenance of the software is essentially the service part of SaaS, so there should never be maintenance charges and since most SaaS is "user-ready" at sign up, there should be no implementation or set-up fee (although some SaaS vendors may offer implementation professional services for an additional cost).	
❑ If there are limits or restrictions on volume of use or users of the Services, there is a mechanism for addressing "overuse."	SaaS vendors usually charge based on either number of users or volume of usage. Many also offer open platforms and self-provisioning of users to make it easier for customers to use the services. The absence of system restrictions on the customer's ability to use the services means that it is possible that the customer use may exceed the customer's committed subscription amount. It is therefore important to have terms that govern how the customer will be charged in the event of that overage. In those situations, it is typical for negotiated pricing to apply to the committed volumes of use or number of users, and online pricing for such "on-demand" use (note that the costs of on-demand usage is also higher for the SaaS vendor because they have negotiated pricing with their upstream vendors as well based on the customer committed amounts).	
❑ It is clear how the charges are invoiced (monthly, quarterly, or annually and in advance or in arrears).	The frequency of payments must be clear. There are a number of different models, but typically, fees that are known, such as flat subscription charges or committed spend amounts are invoiced in advance (annually, quarterly, or monthly), while unknown fees, such as non-committed usage or volume-based charges, are billed in arrears after the reports are generated. If variable usage sensitive fees are billed in advance based on prior period numbers, this can become cumbersome and labor-intensive for both parties in terms of tracking and true-ups and more likely to result in disputes.	
❑ It is clear when/what pricing may change and	Generally pricing set forth on an order cannot change during the term of the order, but pricing may be changed at renewal (which may or may not	

when/what pricing may not change.	be capped or linked to inflation in connection with renewals), and the customer should have the option to not renew when the pricing changes. Pricing that is posted online may be raised from time to time by the vendor. Although not typical in SaaS, any mechanism for capping periodical increases / indexation should be agreed at the outset. In some countries with extremely high inflation, it may be the norm to build inflationary increases into the pricing during terms that extend beyond a year. Change control procedures are not needed to address these in-term price fluctuations.
❑ The terms around renewal are clear.	Many SaaS contracts include auto-renewal as a default. This is beneficial to the SaaS vendor because it saves administrative and selling time. This may or may not be beneficial to the customer depending on the criticality of the SaaS, the maturity of the customer's team responsible for tracking and handling renewals, and the consequences of a failure to take action when there is no auto-renewal (e.g., will the services be turned off or the pricing move from negotiated discounts). Whether or not there is auto-renewal in the agreement, the terms around notices with respect to expiration, cancellation (if any), renewal, and renewal price changes should be clear.
❑ The agreement has a mechanism for the customer to withhold payment for a disputed charge without penalty (interest, suspension of service) or for the vendor to correct an invoice – both within a reasonable window after the bill has been issued.	As SaaS is web-based, the vendor should be able to automate and continuously monitor the customer's use of the SaaS solution and can automatically bill customers based on that use. Where possible, the vendor should provide equal transparency to the customer, so that the customer can also administer and track usage and is not surprised by bills that reflect any overages. With this transparency of pricing and usage, and clear terms around the pricing of overages, disputes are less likely to arise in a SaaS and the window for disputes can be quite short. In addition, there is usually no need for the contract to include customer audits of vendor's billing or vendor audits of customer usage (although if usage information is held only by one party, there should be a requirement for that information to be shared for review upon request).
❑ Indirect purchases may need to be addressed.	One of the prevalent purchasing mechanisms for SaaS is the ability to purchase through a marketplace. These are offered by all of the big CSPs as well as by many SaaS vendors and other specialized marketplaces. The parties may want to include terms in the agreement that enable the customer to purchase directly or through a marketplace or through a reseller at different times in the relationship. Such a clause would state that the terms of the agreement would apply to those purchases except for the clauses that are no longer applicable to the direct relationship such as invoicing.

Issue	Concepts in SaaS Contracts	Concepts Typically Not in SaaS Contracts
D. There are appropriate mechanisms to protect the SaaS solution and the customer data.	❑ Security ❑ Privacy ❑ Transparency in where the data is processed ❑ Confidentiality ❑ Safeguarding the SaaS	❑ Unique customer security requirements
Checklist	**Notes**	
❑ There is an obligation for the vendor to provide security and a commitment that the security will not be decreased during the term but rather adjusted as changes in risks take place.	The multi-tenant nature of SaaS means that there is only one security framework for all of the customers on the SaaS platform; it is architecturally impossible for each customer to have their own security protocols. Therefore, the customer security team should review the vendor's current security protocols and decide whether they are sufficient for the customer's needs, and the agreement should require that the overall security will not be decreased during the term. In addition, a mature SaaS vendor is likely to have ISO certifications and/or SOC audits; having basic obligations to adhere to these industry standards in the contract is reasonable in a SaaS agreement. Given the pace of technology and of new risks from bad players, vendors should be required to continue to adhere to these standards as they change from time to time.	
❑ There is an obligation for the vendor to provide information that will enable the customer to assess the vendor security measures.	The contract should include one of the following means for assessing the vendor security: (1) a commitment to make details around their security measures available through a secure portal for easy access by the customer's security team at any time; (2) the annual provision of key security information through a SIG or a QAIC form, provision of standard industry certifications and reports (e.g., SOC or ISO), or a response to a security questionnaire; or, where either of the preceding is not possible, or (3) a security audit right.	
❑ There are obligations on both parties to comply with all laws and regulations that apply to the international movement, storage and processing of personal data.	Most SaaS vendors have a standard data processing agreement that is designed to be in compliance with privacy laws and regulations and that reflect the actual processes the vendor follows for meeting those laws and regulations. Some SaaS vendors have product options that allow for data residency in one jurisdiction, but many do not have that option. If it is not an existing option, the vendor will likely not be able to create that option for an individual customer (and if it can, it may be at the expense of functionality or potentially only at a much higher cost). For vendors that do not have a European data residency option, many will be able to provide their pre-prepared transfer impact assessments to customers. The vendor will look for the customer to make commitments around not inputting personal data without having the proper consents and, depending on the nature of the services, may also include limits on the inclusion of any personal data or specific types of personal data. The parties should also have clarity as to how long the inputted data and the outputs will be stored by the SaaS vendor. Some vendors have set retention periods for their product(s) that are shorter than the term; in other cases, the data may persist through the full term of an order or longer. To comply with	

	privacy laws or otherwise, the customer should also be able to make data deletion requests outside of any specified deletion period.
❑ There are confidentiality obligations on both parties.	Like most other contracts, SaaS contracts include standard confidentiality obligations. Confidential Information relating to SaaS may include the vendor's security information, the SaaS architecture, product roadmaps, the customer's usage data, performance data of the SaaS, and information related to customer's internal systems and operations. There should be a general obligation to delete confidential information at the end of the term (since information is not generally exchanged in hard form, a requirement to return the confidential information may not be practical). Note, deletion of account data and customer data may be addressed separately from other confidential information as the deletion of customer data is generally addressed in connection with post termination access rights and survival (see Section G, below) and occurs subsequent to any post-termination access right for customer's retrieval of the data. Account data may need to persist as long as any terms of the agreement survive.
❑ There is a mechanism for the vendor to protect the SaaS solution from violations of use restrictions.	As addressed in Section A, above, there are use restrictions imposed on the customer, and some of those restrictions relate to maintaining the security and integrity of the SaaS. The vendor must have the ability and the right to suspend customers and/or their users when those use restrictions are not adhered to and to do so without advance notice in the case of imminent harm to the customer, the SaaS itself, or other customers.

Issue	Concepts in SaaS Contracts	Concepts Typically Not in SaaS Contracts
E. There are no unexpected transfers of ownership.	❑ Data, services and feedback ownership	❑ License copying/rights beyond just right to use ❑ Work for hire
Checklist	**Notes**	
❑ Customer owns its inputs and outputs.	SaaS usually does not provide value to a customer until the customer inputs its own data. This addition of customer data into the SaaS solution should not result in a transfer of ownership of the data. Some SaaS solutions create outputs for the customer based on that data. To the extent the outputs are a derivation based on that data, the outputs specific to that data should also be owned by the customer (excepting feedback and aggregated/anonymized data as addressed below). Note that the outputs are just functions of how the SaaS solution works; they are not deliverables provided in accordance with customer specifications. Even for vendors that provide professional services in connection with their SaaS solution, the work does not generally include deliverables created to customer specifications but is rather the SaaS vendor implementing its own best practices. As such, work-for-hire clauses are rarely appropriate in SaaS engagements unless the professional services are outside the scope of the SaaS application or software.	
❑ Vendor owns the services, feedback, usage data and aggregated and anonymized data sets.	The SaaS solution should not change ownership from the vendor to the customer in connection with customer's use of the SaaS. Feedback is customer's identification of changes that should be considered for the SaaS solution and should be owned by the vendor so that the vendor can make improvements based on that feedback. The scope of feedback to be owned by the vendor should exclude customer's confidential information. In addition, like all businesses, SaaS vendors monitor the consumption of their services, including how many times users are logging in, how users are navigating when they are in the solution, what uses are the most frequent, and other data on customer use of their solution ("usage data"). SaaS vendors rely on the feedback and on usage data to improve their products, and the whole marketplace benefits from those continual improvements. Last, as discussed in Section A, customers are often looking for insights that are derived by the vendor through the analysis of aggregated and anonymized data across its customers. Although the customers own their individual inputs the aggregated data set is owned by the vendor.	

Issue	Concepts in SaaS Contracts	Concepts Typically Not in SaaS Contracts
F. Risk apportionment is balanced.	❑ No indirect or consequential damages ❑ Uncapped liability for gross negligence and willful misconduct ❑ Capped liability for simple negligence ❑ Secondary caps for high-risk areas such as data breaches ❑ Intellectual property and misuse indemnifications ❑ Insurance	❑ Liability or indemnity around employee issues or physical harms ❑ Liquidated damages

Checklist	Notes
❑ Neither party is responsible for indirect or consequential damages or for lost profits, revenues, goodwill, except with respect to types of liability that cannot be excluded by law (dependent on jurisdiction).	As with most commercial contracts, risk allocation does not include liability for indirect or consequential damages. Exceptions to this exclusion are where the governing law prohibits that exclusion. For many jurisdictions, liability for gross negligence, willful misconduct, and fraud cannot be contractually limited. When in doubt and to have flexibility, you can include the proviso "unless contrary to laws" within the exclusions clause.
❑ Uncapped liability is limited to egregious harms.	As with most commercial contracts, uncapped liability is also restricted to gross negligence, willful misconduct, and fraud. Uncapping liability for other potential damages could make the contract financially unbalanced.
❑ Standard liability for direct damages capped at a market rate.	The predominant standard for direct damages for SaaS is 12 months fees paid or sometimes paid or payable. Although based on bargaining power and the potential risks for that service, there may be a low number multiplier (e.g., 1.5). Sometimes risk grows proportionate to the volume of use; in other cases, there may be a risk of damages the first day of use. In the latter situations, if the fees are not paid upfront, you may negotiate a direct damages floor of a specific dollar amount or, for caps based on fees paid in the past X months, an amount equal to X times the monthly average spend until that initial X month period has passed.
❑ High-risk areas may have a secondary cap.	Where the nature of the services includes risk areas with the potential for high damages exposure, such as breaches of security obligations that result in the disclosure of personal information, the application of super caps / increased caps for certain types of losses or damages such as those resulting from confidentiality or data breaches are not uncommon. In fact, data related risks are arguably some of the most widely discussed types of liabilities in SaaS, especially for regulated customers. Generally, the amount of the secondary cap should relate to the nature of the SaaS solution, the value of the benefits it provides, and the sensitivity of data each party expects to be inputted into the

	SaaS solution. In setting a cap amount, keep in mind that the overall goal is to mitigate the risk that is specific to the engagement rather than risk attached to the existence of the data itself. The amount of exposure held by the SaaS vendor should have some reasonable degree of proportionality to the spend with the vendor, the decrease in risk and savings the customer is generating by using the SaaS, and the amount of control the customer has in protecting that data itself (for example if the vendor includes tools the customer can use to hash or omit specific types of data). For these reasons, unlimited liability is usually not acceptable and not market practice.
❑ The indemnities reflect the claims that each party is in the best position to defend, and which are independent of the other party's actions.	It is typical for SaaS indemnification clauses to include an indemnity by the SaaS vendor for IP claims (with standard carve outs for things outside of the vendor's control such as use that doesn't comport with limits of the agreement) and an indemnity by the customer for claims arising from its own systems and other services it connects to the SaaS, the data that it inputs, and for bad acts with respect to the SaaS platform.
❑ Vendor is obligated to maintain insurance, including for cyber security and errors and omissions.	Particularly for a smaller vendor, cyber security and errors and omissions insurance coverage will cover the areas of greatest risk arising from the vendor's fault which can provide the customer a safety net to cover applicable damages, at least to a certain degree.

Issue	Concepts in SaaS Contracts	Concepts Typically Not in SaaS Contracts
G. Termination rights are clear.	❑ Termination for Breach ❑ Limited Refunds/Fees Owed ❑ Termination of Rights ❑ Post-Termination Access ❑ Deletion of Data	❑ Convenience Termination ❑ Termination Assistance ❑ Reversibility ❑ Migration

Checklist	Notes
❑ A refund will be provided in the event of termination by customer for vendor's material breach or a termination by vendor in connection with an IP claim; in all other cases all amounts under the order become due upon customer termination.	The termination of the agreement only excuses customer payments where the termination is due to the vendor's acts (generally an IP infringement claim where the vendor is unable to keep providing the service or where there is a material breach by the vendor). As pricing is usually based on committed terms, most SaaS agreements do not include a customer right to terminate for convenience. Customers that are looking for flexibility may be able to select pay as you go or month-to-month subscription options, which are at a higher cost. In some cases, a termination for convenience right may be available with either the payment of all the remaining committed amount plus any overages to date or with a negotiated early termination fee.
❑ Customer has the right to access the data in the services for a limited period after the end of the agreement to retrieve the data.	The customer must have an opportunity to extract its data from the SaaS solution. In some jurisdictions, this is also required by applicable law. While this can be done during the term, at the end of the contract - especially in the case of a termination as opposed to expiration - the customer may need additional time to access the services for the purpose of extracting the data. This access should be limited to extracting the data and not otherwise using the services or adding to the dataset. Continuing use of the SaaS post-term may be subject to a penalty since the rights have ended and, therefore would be in breach of the right to access and, perhaps, subject to the vendor's on-demand pricing. Customers should be operationally aware of this potential and take the necessary steps to de-activate any connections that might be automatically sending data to the SaaS solution. The access to data and the ability to export it will typically be the only transition assistance that the SaaS vendor will provide to the customer.
❑ After the post-termination access period, customer has no right to access the services.	SaaS revenue is based on payment for access. Once any agreed upon access period has ended, the SaaS vendor should not be providing free access.
❑ Vendor will delete the data from the services.	Both the vendor and the customer have an interest (and often a legal obligation with respect to personal information) in the vendor not retaining the customer data in the service indefinitely from both a security and a cost perspective. In some cases, the SaaS product already has a data retention period that will naturally result in the deletion of data from the services within a reasonable period. In other cases, retention may continue indefinitely in the absence of specific action by the vendor, and the parties will have to specify the deletion period.

IV. Applicability of the World CC Contracting Principles to SaaS

Below is each WorldCC Contracting Principle with an indicator as to whether or not it is applicable to a SaaS contract along with an explanation as needed.

WorldCC Contracting Principle	SaaS Application
1. Alternative Dispute Resolution	⊘ As SaaS should be a low-touch engagement model, contracts tend to be shorter and do not include extensive dispute resolution terms; although for strategic engagements, there may be pre-litigation escalation procedures.
2. Assignment and Novation	✓ This Principle is applicable to SaaS agreements.
3. Compliance with Laws	✓ This Principle is applicable to SaaS agreements.
4. Confidential Information	✓ This Principle is applicable to SaaS agreements.
5. Customer Audit of Suppliers	✓ This Principle is applicable to SaaS agreements. Applying the guidance under this Principle to SaaS, customers should only need an audit right if the SaaS vendor does not already provide access to the financial information needed to verify the billing calculations and access to redacted security reports and security certifications needed to assess security. If the usage information tied to billing is not available to both parties then the party with the information should have an obligation to make it available, subject to review.
6. Data Security and Privacy	✓ This Principle is applicable to SaaS agreements. Note, however, data export or data localization restrictions are generally not available in SaaS, except to the extent the SaaS vendor has an "in-region only" option for data residency.
7. Force Majeure	✓ This Principle is applicable to SaaS agreements. Note, however, that vendors should have obligations to maintain (along with their suppliers) up-to-date business continuity and disaster recovery plans that will mitigate the impact of any Force Majeure Event.
8. Indemnification of Third Party Claims (Excluding Intellectual Property Claims)	✓ This Principle is applicable to SaaS agreements. Note, however, because SaaS is web-based, the scope of indemnity obligations should be reviewed for applicability (e.g., indemnification for personal injury is not particularly relevant if the parties never deal with each other in person).

9. Insurance Coverages	✅ This Principle is applicable to SaaS agreements. Note, however, because SaaS is web-based, the scope of insurance coverages should be reviewed for applicability (e.g., motor vehicle liability is unlikely to be relevant). For vendors that offer SaaS to large customer bases, it may not be practical to have each customer as a named insured under the policies.
10. Intellectual Property Rights and Indemnification for Third Party IP Claims	✅ This Principle is applicable to SaaS agreements. However, applying the guidance under this Principle to SaaS, customized software development is not the norm in SaaS; therefore, work-for-hire clauses would only be relevant, if at all, as part of professional services that are tangential to the SaaS and that include customized deliverables.
11. Liability Caps and Exclusions From Liability	✅ This Principle is applicable to SaaS agreements. Note, however, the application of super caps usually apply to data breaches and, on a growing basis, to breaches of confidentiality. Liability for items that are inapplicable to SaaS, such as bodily injury, property damage, or employer liability are not appropriate exceptions to the cap, except in jurisdictions where those liability types cannot be excluded or limited.
12. Managing Price Volatility	➖ SaaS agreements are typically relatively short; unforeseeable, extreme external conditions don't usually dramatically affect prices; and multiple other sources exist in the market. Therefore, applying the guidance under this Principle to SaaS, these terms are generally not applicable, although there may be pricing increase caps in connection with auto-renewal clauses.
13. Non-Solicitation	🚫 SaaS is a low-touch engagement model. Applying the guidance under this Principle to SaaS, non-solicitation requirements are normally not included.
14. Payment Terms	✅ This Principle is applicable to SaaS agreements. Note that additional assurances and set-off rights are atypical in SaaS agreements.
15. Prices and Charges	✅ This Principle is generally applicable to SaaS agreements.
16. Requirements for Accessing the Other Party's Assets	🚫 SaaS personnel do not typically access customer's systems or premises, and they support not just one customer, but many. This Principle is not generally applicable to SaaS.
17. Service Level Agreement Remedies	✅ This Principle is applicable to SaaS agreements. Note that service level commitments and credits, if any, are typically limited to meeting availability standards.
18. Step-In Rights	🚫 Given the technical aspects of how SaaS is delivered and the fact that the software and systems are made available to multiple customers, step-in rights cannot be provided.

19. Sub-Contracting	⊖ Most SaaS solutions incorporate technology from other vendors, and, therefore, SaaS vendors cannot give individual customers control over the technology or subcontractors being used for the SaaS solution. The exception to this is with respect to the addition of new subprocessors (from a data protection perspective), for which SaaS vendors will provide a limited customer objection period which could translate into an early termination right of the subscription. Vendors should be responsible for ensuring that their contracts with their subcontractors contain confidentiality obligations and reasonable security measures, although those will not be specific to any particular customer's requirements.
20. Suspension Rights	✓ This Principle is applicable to SaaS agreements with respect to vendor suspensions. Given that SaaS is based on a right to access the service, this is particularly relevant and typically comes with a short prior notification mechanism unless the suspension is necessary to protect the integrity or security of the SaaS platform against imminent harm.
21. Termination Assistance	⊘ To the extent the SaaS solution enables export of data, the contract should contain provisions on data portability post-termination for a limited period of time contractually agreed, but bespoke exit plans is a concept not generally aligned with a SaaS offering.
22. Warranties	✓ This Principle is generally applicable to SaaS agreements; however, because SaaS is delivered "as is", the express warranty is usually limited to the SaaS product functioning in accordance with the documentation, rather than meeting customer-specific specifications or quality controls, and the warranty should persist for the term of the contract. The primary risk for SaaS is a lack of availability which is typically addressed through a standalone clause, rather than in the warranty section, which both defines and provides remedies for availability failures.