

Moving to a SaaS Business Model? 5 Legal Issues to Consider

Commercial and Contracts

Information Governance

Career Development

Technology, Privacy, and eCommerce



Banner artwork by jannoon028 / *shutterstock.com*

When a software vendor makes the business decision to migrate from an on-premise software license model to a cloud-based software as a service arrangement (SaaS), there are several important legal issues to consider, including how changes to the business model will impact the vendor's agreement with its customers. Let's first review the basic differences between on-premise software and SaaS.

On-premise vs. SaaS

Under an on-premise model, the vendor grants a copyright license to its customers that allows them to download, install, and use the vendor's software on the customer's computers. In exchange for this license grant, the customer pays a license fee to the vendor. Under a SaaS model, the vendor's software is hosted in the cloud and customers access it remotely: the customer does not download, copy, or install it. As a result, a SaaS arrangement does not require a copyright license, because the customer never gets a copy of the vendor's software. Instead, the SaaS vendor grants permission to access the software remotely, simply called an "access right."

In addition, a SaaS arrangement differs from a traditional on-premise one in the following ways:

- SaaS is akin to a time-limited, rental, or subscription arrangement, whereas on-premise often

involves a perpetual right to use the software.
- SaaS enables vendors to easily update, upgrade, perform bug fixes and maintain their software without involving the customer.
- SaaS eliminates time-consuming and costly on-site installation at the customer location, which was often required for an on-premise arrangement, saving both parties time and money.
- In a SaaS model, the software is stored and maintained remotely, so the customer no longer needs servers and IT personnel to manage the on-premise software, reducing customer costs.
- In a SaaS model, the customer's data may be processed, transferred, and stored in the cloud and responsibilities for ensuring the security of such data are often negotiated between the vendor and customer. In the on-premise model, aspects concerning the security of the customer's data are usually the customer's responsibility.

5 legal issues to consider when migrating to a SaaS model

Given the fundamental differences between the on-premise and SaaS models, vendors migrating to a SaaS business model should not use their legacy software license agreement, as it is no longer appropriate. Instead, vendors should employ a SaaS subscription agreement, which, among other things, addresses the following considerations:

1. Access rights

Under a SaaS subscription agreement, the software vendor grants its customer a right to access the remotely hosted software. In exchange for this access right, the customer pays a subscription service fee. For example, Netflix employs a SaaS business model that provides on-demand movies via their remotely hosted software to which customers gain access in exchange for paying the subscription service fee.

> Under a SaaS model, the vendor's software is hosted in the cloud and customers access it remotely: the customer does not download, copy, or install it.

2. Authorized users

The individuals who may lawfully access the remotely hosted software are the customer's "authorized users." Their access and usage are subject to the terms of the SaaS subscription agreement. Accordingly, authorized users should be clearly defined in the agreement, and they may include the customer's employees, affiliated companies, and designated subcontractors. Typically, the vendor will require the customer to assume responsibility for ensuring that all authorized users abide by the terms of the SaaS subscription agreement.

3. Hosting provider implications

Unless vendors have their own servers to host their software, they will need to contract with a hosting provider – such as Amazon Web Services or Akamai – to host their software before they may offer a SaaS option to customers. The terms of the hosting provider agreement will likely inform how certain provisions in the vendor's SaaS subscription agreement are presented to the vendor's customers. For example, the geographical location of the hosting provider's servers will likely dictate which data privacy laws apply to data being processed, transferred, or stored when customers access the SaaS. Such data-related laws and regulations vary greatly around the globe. Some impose strict requirements and liabilities, so software vendors should consider this aspect when selecting a hosting provider.

> The geographical location of the hosting provider's servers will likely dictate which data privacy laws apply to data being processed, transferred, or stored when customers access the SaaS.

The hosting provider's agreement may also set out access-related parameters. For example, hosting providers generally do not guarantee 24/7 availability, and many observe preplanned technical maintenance periods when their servers – and anything hosted on them – will be inaccessible to the vendor and the vendor's customers. Therefore, software vendors should ensure that the availability metrics they provide to customers in their SaaS-related service level agreements (or SLAs) synchronize with those the hosting provider offers.

4. Vendor recourse

Under an on-premise software arrangement, the customer has a copy of the vendor's software, so vendors cannot easily stop the customer from continuing to use it if the customer breaches the agreement. However, if a SaaS customer breaches the agreement terms, a vendor may easily suspend their remote access until the customer is back in compliance. This leverage, and the conditions under which the vendor may impose it, should be stated in the SaaS subscription agreement. In addition, as in all commercial agreements, the vendor's SaaS agreement should include legal recourse and remedies in the event the customer breaches.

5. Data-related issues

Issues relating to data ownership, data related liabilities, and privacy and security should be addressed in the SaaS agreement, because customer data is often transferred, processed, or stored in the cloud when the customer accesses the software. In addition, the SaaS agreement should address each party's respective responsibilities and liabilities if a data breach occurs, noting that certain data-related laws and regulations may automatically govern certain aspects of a data breach.

Finally, it is important to note that, just like most other commercial agreements, a SaaS subscription agreement should include standard commercial terms such as:

- Intellectual property ownership concerning the SaaS, brands, logos and data;
- Warranties and representations;
- Indemnification and limitations of liability;

- Confidentiality;
- Payment and renewal terms; and
- Dispute resolution.

From the customer's perspective

Vendors may wish to consider a few key issues from the customer's point of view, so they may create an established approach for responding to and addressing customer requests relating to the SaaS arrangement. These issues include:

- **Data security** — Do the vendor's technical safeguards align with the customer's data security requirements?
- **Performance metrics** — Does the SaaS agreement's SLA include uptime and performance metrics with respective remedies if such commitments are not met in a timely manner?
- **Termination rights** — Under what circumstances may the customer terminate the agreement, particularly if the proposed term of the SaaS arrangement is three years or longer?
- **Contract renewal** — Does the SaaS agreement auto-renew? If so, how much flexibility will the customer have at the time of renewal?
- **Fee caps** — Are the vendor's fee increases capped?
- **Compliance guarantee** — Does the vendor agree to comply with applicable laws, as those may evolve during the term of the SaaS agreement?

Along the same lines, the SaaS vendor's counsel may want to consider working together with their internal business partners to create a playbook on how to address such concerns before negotiating a SaaS deal with a customer. Establishing a playbook will enable the vendor to close customer SaaS deals with greater efficiency and achieve more consistent deal terms across its customer base.

In closing, the best approach for software vendors contemplating migrating to a SaaS business model is to first understand how SaaS deals differ from on-premise software license arrangements, and then, to amend their customer agreement accordingly in order to capture the full scope of a SaaS arrangement.

Billie Munro Audia



Partner and Retail, Marketing & Media Practice Area Leader

Outside GC

Billie Munro Audia writes the Contracts Corner column, partnering with in-house counsel, for *Corporate Counsel Now*. She is a partner with Outside GC, the provider of choice for on-demand general counsel services, and she leads the firm’s Retail, Marketing & Media Practice. Billie has 20+

years of commercial legal experience in the retail, media, and technology sectors, including 7 years in London as European General Counsel for two Silicon Valley technology companies and 4 years in San Francisco as the Director of Commercial Transactions for Gap, Inc. At the beginning of her career, she was an associate with Covington & Burling.

Ana Liggio



Assistant General Counsel

Catalent Pharma Solutions, LLC.

Ana O'Keefe Liggio is an Assistant General Counsel with Catalent Pharma Solutions, LLC., a global provider of delivery technologies, development, drug manufacturing, biologics, gene therapies and consumer health products. Ana is a healthcare, tech, and life sciences attorney, with over 15 years of experience advising clients on commercial matters such as contracting, data privacy and security, dispute resolution, and compliance. Ana is a member of the Association of Corporate Counsel and frequently participates in ACC conferences.