7 Key Privacy Provisions For Software Delivery Agreements

By **Lori Ross** (December 6, 2022)

Lori Ross

Privacy and data protection issues continue to be a top priority for many businesses, especially in light of the stiff financial and reputational consequences that can result from a finding of noncompliance.

Recently, California Attorney General Rob Bonta announced his intention to pursue more enforcement actions under the state's two privacy laws, including by taking aim at software as a service, or SaaS, providers who fail to provide appropriate privacy notices or give consumers the option to opt out of having their information sold.

Meanwhile, European regulators have already issued massive fines against SaaS operators Amazon Web Services Inc., Google LCC and Clearview AI Inc. for failing to comply with privacy requirements related to the processing of customer data.

Given the rising popularity of the SaaS model of software delivery, it will be incumbent upon SaaS providers to understand the myriad privacy and compliance considerations relating to customer data and take steps to address them in their customer agreements.

Below, we explore seven key data-related provisions that should be included in a provider's SaaS subscription agreement.

1. Ownership of Data and Usage Rights

Both sides of a SaaS arrangement have ownership rights that should be clearly defined in the subscription agreement.

A provider typically owns the intellectual property rights in the underlying platform, as well as any content that is generated to support performance of SaaS services.

Meanwhile, customers will own the data that they input into a SaaS product, along with any data generated as a result of this input. By carefully defining key terms like "customer data" and "SaaS platform data" or "provider data," these ownership rights will be clearly delineated.

Additionally, since some providers may need customer data from time to time, the agreement should grant providers usage rights over such data, subject to any limitations specified in the agreement or imposed by applicable regulations such as the California Consumer Privacy Act and the upcoming California Privacy Rights Act.

Generally, usage rights are limited to account administration and analytical, statistical or product improvement purposes and allowed only if the data is anonymized.

Finally, when a SaaS agreement contains a statement of work and includes the provision of professional services as part of a suite of services, ownership rights to the finished product should be defined.

Although a provider may agree to characterize new products as works for hire in order to preserve the customer's ownership of them, the rights to the provider's underlying program

or background intellectual property should be clearly identified as belonging to the provider.

2. Protection of Customer Data

Data privacy and data security are two different things. In addition to provisions relating to data privacy and data ownership, the SaaS agreement should also address data security.

Although no provider can guarantee 100% security, customers often seek assurances that their data is secure, usually by requesting a detailed description of the provider's technical and organizational measures designed to protect data.

Given the seriousness of security threats, various regulatory regimes mandate that SaaS providers have adequate technical and organization measures in place, including the General Data Protection Regulation in the EU, the British post-Brexit regime, and U.S. federal and state laws such as the Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, California's CCPA and CPRA, and other state legislation.

3. Audit Rights

Some SaaS customers may request the right to audit a provider's systems to ensure an appropriate level of protection is in place.

Aside from those required to grant audit rights under the GDPR, providers should consider offering less intrusive alternatives such as agreeing to provide audit reports — System and Organization Controls 1 and 2 — or independent third-party assessments.

If a provider is subject to the GDPR, these rights should be limited as much as possible within the GDPR guidelines.

4. Storage and Processing of Data

The location where customer data will be stored, accessed or even just transferred determines which regulatory scheme applies to a SaaS arrangement, as well as what type of technical and organizational measures are required.

Under the GDPR, the location of the provider is irrelevant. The GDPR applies whenever the data of EU residents is routinely handled.

Even a U.S. company utilizing U.S.-based employees will be subject to the GDPR if it handles EU resident data in any meaningful way, including the transfer, processing, use or storage of EU resident data.

5. Retention of and Access to Data

A software provider's basic data retention policies with respect to customer data should be spelled out in the SaaS agreement. Under generally accepted data privacy principles, data is kept no longer than necessary to fulfill the purpose for which it was collected.

Most providers do not want to hold on to customer data once the relationship has ended. That said, there are some generally accepted exceptions to the practice of deleting data as quickly as possible.

Retention may be necessary or appropriate if the data is needed for purposes of completing

transactions, upholding legal obligations, maintaining security and existing functionality, protecting free speech, conducting research, and for internal, expected and lawful uses by, or legitimate interests of, the provider.

On a related note, many regulatory regimes now give data subjects — i.e., any individual whose data has been included as a part of customer data — rights to access, delete and correct their data.

SaaS providers should ensure that the primary responsibility and obligation to respond to any data subject access requests, or DSARs, rest with the owner of the data — their customer.

Since SaaS providers offer a multitenant solution, it is not possible, or even technologically or physically possible, for the provider to respond to DSARs from all of the individuals whose data may be involved.

Moreover, a SaaS provider should not have the responsibility to respond to DSARs since it does not have access to or insight into its customers' content.

6. International Transfers of Data

When a customer's data includes EU or European Economic Area resident data — including the U.K. and Switzerland — a data processing agreement, or DPA, between the provider and customer is required. A DPA essentially tracks the GDPR and other applicable data privacy laws.

A DPA may include standard contractual clauses or binding corporate rules if chosen as the mechanism for protecting international data transfers when the target jurisdiction is seen as not providing adequate protection of data.

DPAs are increasingly being used even when data does not cross international borders.

7. Liability for Issues Related to Data Loss and Data Breach

Issues relating to data loss and data breach loom large in SaaS arrangements. Typically, providers will disclaim liability for these types of losses in a SaaS agreement.

If a provider is willing or is forced due to its bargaining position to accept liability for such issues, liability should be capped at some multiplier of the contract value and limited in scope to only those losses caused by the provider's product while data is under its control.

Many SaaS providers obtain cyber liability insurance as a means of mitigating their liability risk.

Conclusion

The global SaaS market was valued at $143 billion in 2021 and is expected to reach $720 billion by 2028, according to some estimates.

With this forecasted growth in the market, more and more customers are likely to turn to SaaS providers to help get business done, and in doing so, huge volumes of the data will be accessed, manipulated and analyzed.

It is therefore crucial that SaaS providers clearly delineate all rights and responsibilities with respect to such data in their customer agreements.

Lori S. Ross is a partner at Outside GC LLC.