



Privacy “Software as a Service” Agreements and the Transfer of Personal Information

by Martin C. Finestone

Martin C. Finestone, Associate Business Law
Waterloo Region
(519) 575-7533
martin.fineston@gowlings.com

Martin is a member of both the business law department and Technology Group. He provides advice on a variety of technology and non-technology clients on general corporate and commercial matters, financings and M&As. He also assists clients by negotiating and drafting licensing, content, terms of service and other agreements, and advising clients on Internet-related issues.

If your organization seeks to engage the services of a “software as a service” (SaaS) provider and will be transferring the personal information of your customers and/or employees to the SaaS provider’s servers, you should consider the privacy law implications before entering into an agreement for services (Services Agreement).

Listed below are a number of issues, questions and possible contractual measures concerning several of the privacy law implications to consider when planning for and negotiating a Services Agreement. (Please note that this article is not intended to provide an exhaustive list of privacy law issues and considerations on the subject, nor is it intended to provide legal advice or to replace consultation with a legal professional.)

Preliminary Considerations

Prior to entering into a Services Agreement with a SaaS provider, consider taking some or all of the following steps:

- Ascertain whether your organization has permission to transfer and/or outsource the processing of the personal information of your customers or employees.
- Review the status your organization’s privacy policy. For instance, do you have consent to transfer information that you have already collected? Will amendments be required to your privacy policy in order to reflect the

proposed new arrangement with the SaaS provider?

- Assess the legislative and regulatory requirements for protecting the data that is in your care and for which you are accountable. For example, if your organization is in, or provides services to, the financial sector, consider whether you must comply with the Office of the Superintendent of Financial Institution’s rules on IT outsourcing, and how those rules would affect the SaaS relationship.
- Consider carrying out a due diligence review of the SaaS provider’s operations, including a review of their information security procedures and practices.
- Consider evaluating the SaaS provider’s data breach response plan and policy as part of the due diligence process.

Substantive Considerations

The following are suggested questions and factors to weigh when approaching the drafting of the Services Agreement:

- The Services Agreement should clearly reflect all parties’ understanding of the SaaS provider’s security obligations. This can be accomplished either by specifically setting out the required practices and procedures to which the SaaS provider must adhere or by specifying compliance with other standards that are measurable.

- Should the transfer of data be restricted to servers in specific jurisdictions? For example, should the transfer to servers in the United States be prohibited?
- Will the Services Agreement contain limitations on the SaaS provider's ability to subcontract services?
- If subcontracting is to be permitted, what rules will you put in place to limit the use of subcontractors and their access to your data?
- Acceptance testing of information security procedures may be appropriate in the context of your use of the SaaS provider's services. If so, the Services Agreement should clearly set out who will be testing the information security procedures and practices for compliance (e.g., your organization, auditors, the SaaS provider under your supervision, a third party, etc.). The Services Agreement should also set out what will happen if acceptance testing fails, such as deferral of payment or the right to terminate the Services Agreement.
- Will you require that the SaaS provider be certified in accordance with one or more accepted IT standards? If so a representation, warranty and covenant to this effect should be requested to be included in the Services Agreement.
- Is it appropriate or necessary for the SaaS provider to have insurance coverage? This will largely depend on the value and sensitivity of your data and the severity of your organization's legal obligations and exposure to liability in the event of a security breach. If insurance will be required, consider what the nature and scope of the coverage will be. Determine whether the SaaS provider's existing coverage will be sufficient and whether their current policy covers damage from security data breaches.
- Consider restricting the SaaS provider's access to personal information to a limited number of people within their organization.
- Consider the relevant remedies in the event of a data breach. Should damages or other remedies resulting from a breach of the SaaS provider's data protection obligations be excluded from any limitations of liability provisions?
- Will it be necessary to mandate that the SaaS provider comply with your organization's privacy practices? If so, ensure that the Services Agreement entitles you to sufficient audit rights to measure the SaaS provider's compliance with those and the other practices to be set out in the Services Agreement.

Data Protection Considerations

- Include a provision in the Services Agreement requiring mandatory disclosure by the SaaS provider of any known security breaches.
- Consider what sort of organizational or system safeguards for the SaaS provider will be appropriate in the circumstances. For example, consider limiting access to printing, storage devices and other means of communication or copying of data.
- Consider mandating the use of encryption technologies for sensitive and personal information for which your organization is responsible, so that the SaaS provider's employees cannot see or understand the data.
- Should the SaaS provider's employees, who will have access to your data, enter into a specified form of confidentiality agreement?



“Consider mandating the use of encryption technologies for sensitive and personal information for which your organization is responsible.”

