A Guide to Select Supply Chain Issues in a SaaS Contract
Timothy M Banks, nNovation LLP

Software as a service (SaaS) is frequently built on a technology stack or supply chain with multiple players. Even the simplest solution may run on Amazon Web Services (AWS), Google Cloud or Microsoft Azure. More complex SaaS platforms may integrate numerous third party solutions. In one sense, tackling the supply chain should be as easy as requiring the SaaS vendor to flow contractual provisions in the customer contract back through the supply chain. In practice, however, the SaaS provider may have limited commercial power to do so. Even if the SaaS provider is inclined to take on that challenge, it is frequently impossible to determine whether it has actually done so because the terms of the negotiated agreements with upstream suppliers will be confidential.

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
Scope			
Data coverage	Only covers personal data / personal information. Only covers data that is processed on behalf of customer, which likely does not include data collected during support or account information. Excludes usage data.	Personal data is one slice of the data that the vendor wants to protect. It is important, therefore, that the confidentiality and security provisions extend to all data, including data that the vendor might "control" such as data collected during account registration, support calls or that is related to usage of the service.	Contractual: Expand the data protection terms (such as a data protection agreement or addendum) to cover all of the customer data processed on behalf of the customer. Ensure that the confidentiality terms cover data collected during support calls and account registration. Add specific terms with respect to the handling and use of usage data.
Jurisdictional scope	Only applies to data subject to the EU General Data Protection Regulation (GDPR) and UK. May have California provisions for California Consumer Privacy Protection Act.	Canadian data is not protected or only protected to a limited extent. Beware of "lazy" drafting that incorporates by reference terms from the GDPR and not all the terms you need for the contract to be translatable for Canadian	Contractual: Expand definition of data protection laws to include Canadian laws.

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
		privacy laws.	
Flow down of data and jurisdictional scope	Mismatch between the scope of the data protection provisions in the prime contract and those of the subprocessor contracts	For example, the contract with the SaaS provider might extend the data protection provisions to personal information in Canada, but the AWS provisions that the SaaS provider entered into with the hosting provider may only cover EU personal data. The SaaS vendor may not have a sophisticated enough compliance program and purchase power to flow down terms. .	Non-Contractual: Review publicly available data protection terms to understand potential mis-matches. Evaluate practical risks if mismatch is not addressed. Quantify and monitor residual risk, including changes to publicly available subprocessor terms. Contractual: Require vendor to have substantially similar data and jurisdictional scoping terms with its subprocessors and to require subprocessors to have similar terms with their subprocessors. Note: Unless the vendor has a negotiated agreement with AWS, it is virtually certain the vendor does not have adequate privacy protections in place to satisfy Canadian accountability requirements.
Subprocessor Governance Generally			
Authority to engage	General authority to engage subprocessors or (less common) contract is silent	Without understanding the identity of the providers in the supply chain, it is not possible for the customer to fulfill a basic accountability obligation of knowing who is processing the data. It is also impossible to evaluate potential risks in the supply	Non-Contractual: Request list of vendor subprocessors and review publicly available lists of the subprocessors to these subprocessors. (Often available as links in data protection agreements.) Quantify risks associated with current subprocessors, including barriers for transparency with sub-subprocessors.

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
		chain. Invisibility of sub-subprocessors.	Contractual: Require vendor to disclose list of subprocessors and to provide information on sub-subprocessors provided to vendor by its subprocessors (or assist customer in obtaining such information).
Changes to subprocessors	If there is an obligation to notify customer of changes to subprocessors, the notice period is very short.	Vendor does not want to be prevented from moving to a new vendor or having to delay plans for a significant period of time. However, risks in the supply chain may change without customer having the opportunity to evaluate the nature of the risk and make operational changes or seek a new vendor.	Non-Contractual: Engage in ongoing monitoring through subscribing for updates. Monitor changes to sub-subprocessors. Update risk quantification. Contractual: Balance the rights of the vendor with the ability to manage risks. Require vendor to provide a commercially reasonable notice period (e.g. 30 days') before engaging a new subprocessor. Include a termination right that continues after the end of the notice period for a reasonable period of time. This allows the vendor to move onto the new subprocessor notwithstanding customer objections. However, it allows the customer time to finish due diligence and/or move off the vendor's service. It would be exceedingly rare to require the vendor to notify the customer of changes to sub-subprocessors.
Localization			

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
Data transfers	Follow the sun support requires support services in multiple countries	Customers want 24/7 support 365 days a year but don't want access outside to data from outside of Canada or possibility other selected countries	Non-Contractual: Dive deep on how the support will be executed in practice rather than edge cases. Where is support during business hours? Will access to the customer's data be necessary to replicate issues? Will access to data always be pre-authorized? Will support requiring such access be a marker of an escalated issue to be dealt with in-country? If out-of-country support will be in an emergency, is that risk acceptable? What do we know about the clean room practices of the out-of-country support team? Contractual: Require out of country support teams to provide support in clean rooms. Prohibit copying (including screenshots) of any data in customer instance. Require notice of any new support locations in order to evaluate local laws and risks.
	Transfer provisions do not bind subprocessors	Data processing agreement may permit onward transfers from subprocessors, or the data location is unclear.	Non-Contractual: Have quarterly or semi-annual meetings with vendor to review data map. Contractual: Require a flow-down of any data localization restrictions. Require notification of changes to data map or require quarterly or semi-annual meetings to discuss changes or planned

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
			changes.
Data ownership, use and lifecycle			
De-identified Data	Contract permits vendor to de-identify and retain and use customer data as long as it cannot be used to identify customer or an individual	The standard deployed for de-identification by the vendor may be insufficient to transform personal information into non-personal information.	Non-Contractual: Evaluate de-identification methods. The method "pseudonymization" or "anonymization" or somewhere in-between? Obtain information to provide notice to end users / data subjects to get consent. Contractual: If appropriate, permit use of usage data only and require vendor to get consent. Require vendor to represent and warrant that the data will be de-identified to the legal standard required in Canada to make the data non-personal information. Only permit use during life of contract (with consent of the data subject).
Contract permits vendor's use of customer's data for "maintenance and improvement" of the services.	The vendor's use of personal information may be a secondary use.	Customer may require consent of the data subject and ability to opt-out.	Non-Contractual: Obtain a more precise description of the uses up the supply chain to support disclosures. Assess whether the data will be copied into a test/dev environment anywhere in the supply chain. Obtain consent from data subjects. Ensure vendor and its subprocessors can operationalize the withdrawal of consent by a data subject without customer having to delete data from the

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
			operational database. Contractual: If appropriate, only permit use of usage data vs customer content. Only permit use of de-identified data (but see above). Expressly prohibit use in a test/dev environment. Only permit use during life of contract (with consent of the data subject). Require vendor and its subprocessors to cooperate in a withdrawal of consent or anonymize the data used by vendor (without requiring customer to delete data from the customer's instance).
Data destruction	Vendor states that after a certain number of days following the end of the contract, vendor may delete the data.	Vendor is not committing to a deletion period. Vendor does not define whether delete means that the data is incapable of reconstruction. Unclear whether the data may reside in backups and for how long. Unclear how that obligation for destruction flows up the supply chain.	Non-Contractual: Evaluate data destruction methods. Determine whether customer can destroy data prior to termination of contract (e.g. overwriting). Contractual: Require data destruction within a specified period. Ensure definition of "delete" or similar terms means that the data is incapable of reconstruction. Ensure privacy and confidentiality provisions continue until data is destroyed. Require a certificate of destruction that flows up the supply chain.

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
Security Breach			
Definition of security breach	Vendor's definition of security incident only includes unauthorized access to or disclosure of personal information. Security breach definition is phrased in a way that is restricted to the vendor's processing and does not capture subprocessors.	Definition of security breach may be narrower than what customer is required to notify. Vendor may not flow down the same broad definition of security breach as customer seeks from vendor. May be restricted to personal information instead of all of the customer data.	Non-Contractual: Examine publicly available data processing agreements to determine likely scope of subprocessor breach obligations and assess risks of non-compliance with Canadian laws. Use quarterly or semi-annual compliance meetings to determine how vendor is managing breach notification with sub-processors. Contractual: Expand definition of security incident to cover loss of, unauthorized access to (including unauthorized internal access), unauthorized use or alteration of, unauthorized disclosure of customer data. Require vendor to flow obligation through the supply chain.
Timeline for reporting	Timeline for reporting only begins when vendor learns of a confirmed data breach.	The test for reporting by the customer may be lower than a "confirmed" breach. Vendor may not flow-down reporting obligations in the same way, meaning Vendor may not get notification from subprocessor.	Non-Contractual: Examine publicly available data processing agreements to determine likely scope of subprocessor breach obligations and assess risks of non-compliance with Canadian laws. Use quarterly or semi-annual compliance meetings to determine how vendor is managing breach notification with sub-processors. Set-up newsfeeds and subscription

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
			services to monitor news about sub-processors including reports by security researchers. Contractual: Ensure a maximum reporting timeline and require that this also apply to subprocessors.
Root cause and remediation reporting	Vendor's obligation is limited to providing information on the circumstances of the breach as they become available.	Customer may find it difficult to obtain more than high-level assurances that the issues have been remediated.	Non-Contractual Set-up newsfeeds and subscription services to monitor news about sub-processors including reports by security researchers. Contractual Add cooperation requirement and include a requirement to obtain information from subprocessors (likely on a commercially reasonable efforts basis).
Indemnity	Any indemnity against third party claims is limited to vendor's breach of its security obligations.	The vendor's contractual security obligations may not flow down to sub-processor. Vendor may not be liable to indemnify for sub-processor failures.	Non-Contractual: Assess degree to which sub-processor may create a security risk and insure against it. Contractual: Require vendor to assess security of sub-processor's services and use good industry practices in configuring sub-processor's services (if applicable) or requiring sub-processor to adhere to substantially similar security standards having regard to the nature of the sub-processor's services.

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
Data restoration	No commitment to restore data following a breach out of vendor and its subprocessor's backups.	Although data from the vendor might be backed up by vendor or customer, this might not hold true for subprocessor data.	Non-Contractual Determine whether customer can obtain backups of subprocessor data or whether vendor does this. Contractual Ensure data restoration requirement extends to subprocessors.
Audits and Certifications			
Customer audits or reviews	Customer may have the right only to audit or conduct compliance reviews on vendor.	If vendor's solution is built using third-party services components, these components may be the critical pieces (e.g. an infrastructure like AWS).	Non-Contractual Determine whether the subprocessor has third party audits and review them. Determine whether customer has a direct relationship with the subprocessor via a different route in order to obtain information. Contractual Require vendor to use commercially reasonable efforts to obtain information about the subprocessor's controls and to provide that information to customer.
Third party audits or certifications (e.g. SOC 2 / ISO 27001)	Audit may only be of the infrastructure provider.	The vendor may be relying on an infrastructure provider's SOC audit or ISO certification, but this does not cover the services, only certain aspects of the infrastructure.	Non-Contractual Conduct annual reviews of the service provider's controls. Contractual Require the vendor to obtain its own SOC audit or certification in a certain period of time (only works for long relationships). Require vendor to warrant that it uses

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
			the tools made available to the vendor by the subprocessor to protect the data in accordance with good industry practices.
Change Management			
Notice of changes to the services	Vendor may not obtain notice of changes by subprocessors or agree to provide onward notice of changes to customer.	Changes may result in changes to the security or reliability of the services. Changes may require user retraining. Changes may break integrations.	Non-Contractual Understand change management procedures. Arrange for quarterly meetings to review upcoming anticipated changes including any notices form subprocessors of upcoming changes. Contractual Prohibit any changes to the services (including any subprocessor parts of the services) that would result in the diminution of the security or availability of the services. Require reasonable notification of breaking changes or ones that would need employee retraining (time frame depends on the criticality of the services and the amount of time customer would need to take compensating actions.
Regression testing and secure code reviews	Vendor may not conduct regression testing or require secure code reviews for changes throughout the supply chain.	A subprocessor change that introduces a vulnerability or breaking change may result in issues for the services generally.	Non-Contractual Understand change management procedures and whether vendor is able to test subprocessor changes before rolling them out. Arrange for quarterly meetings to review upcoming anticipated changes including

Topic	SaaS Supply Chain Issues	Significance	Possible Mitigations
			any notices form subprocessors of upcoming changes. Contractual Obtain contractual warranty the changes will be tested thoroughly in accordance with good industry practices including regression testing and secure code reviews throughout the supply chain if possible.
Acceptance testing			Non-Contractual Determine whether changes will be automatically promoted or whether they can be tested in a test/dev environment. Contractual Consider liquidated damages for changes that turn out to be breaking changes. Add an acceptance testing period if possible.