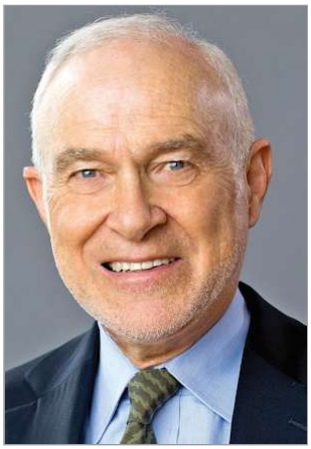
LAW360® Canada

Law360 Canada | 2 Sheppard Avenue East, Suite 1900 | North York, ON M2N 5Y7 | www.law360.ca
Phone: (800) 668-6481 | customerservice@lexisnexis.ca

Office of the Privacy Commissioner: Guidance for contracting with service providers

By **David Young**



David Young

Law360 Canada (October 6, 2026, 2:27 PM EDT) -- The federal Office of the Privacy Commissioner has issued a draft guidance document addressing best practices for organizations contracting with third-party service providers. By its title, "Guidance on Assessing Third-Party Service Providers," the guidance suggests that it should be used by organizations in assessing the qualification of a potential service provider — the due diligence requirement. However, in the broader context, it may be understood as addressing not only the due diligence aspects but also the contracting requirements for organizations' service provider relationships.

To be clear, the guidance focuses on the privacy protection considerations of contracting with service providers where the processing of personal information is a material aspect of the proposed provider relationship. However, while having this privacy focus, the guidance contains important considerations of broader application for an organization evaluating and contracting with a service provider, relevant to, for example, definition of the services, product/service functionalities and performance, and provider roles and responsibilities.

A useful context for this guidance may be seen in the provisions of Quebec's *Law 25* addressing privacy requirements for service provider relationships. While both the current federal law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and the proposed reformed privacy law, the *Protecting Privacy and Consumer Data Act* (PPCDA), stipulate a broad criterion for organizations in qualifying potential service providers — that the organization must ensure by contract or otherwise that the service provider provides a level of protection in respect of the personal information processed by the provider equivalent to that which the organization is required to provide under the law — *Law 25* takes the further step of stipulating minimum contractual provisions.

So, while the draft guidance document talks in terms of assessing potential service providers, it can be understood as directed to fleshing out minimum recommended contractual provisions in order to comply with the statutory rules under PIPEDA and the anticipated PPCDA.

The rationale for the guidance is compliance with PIPEDA's Accountability Principle. That principle states that organizations are responsible for personal information under their control, including personal information transferred to a third party for processing, and must use contractual or other means to provide comparable protection for that information.

The OPC guidance states that, to address these obligations, as a first step before contracting for any products or services that involve processing of personal information, an organization needs to assess a service provider's privacy practices. A rigorous assessment of such practices will assist the organization in meeting its accountability obligations under PIPEDA.

More specifically, such an assessment will: identify privacy and compliance risks and inform strategies for mitigating them; input to the overall vetting of a potential service provider; ensure that there will be accountability for responsible privacy practices, in particular as may be scrutinized by oversight bodies; and indicate terms for inclusion in the contract with the service provider.

The guidance document sets forth a checklist of best practices that it recommends for the assessment process, addressing the service provider's responsibilities. Such responsibilities should be set out in a contract with the service provider. Key items in the OPC's checklist are the following:

How personal data will be used: The assessment should confirm how personal data will be used for performing the contract and in particular that such data will only be used for purposes of the organization's requirements unless expressly permitted to be used for the service provider's own purposes, such as training its systems. If use by the service provider is permitted, the assessment should determine whether any user consent is required.

Identify the core requirements for the service: The organization should assess and identify its core requirements for the product, service or technology being contracted for, relevant to its purposes for collecting, using or disclosing personal information.

Provider's security protocols: A critical aspect of any privacy assessment of a potential service provider is understanding the security policies and practices that the provider has in place. This assessment should include both cybersecurity and physical access controls as well as work environment controls.

Data breaches: The assessment and the resulting contract should address how data breaches will be handled by the service provider, including the respective roles and responsibilities of the organization, the provider and any subcontractors. A minimum requirement will be the obligation of the provider to notify the organization immediately once it becomes aware of a breach.

Cross-border transfers: If the service provision will be performed at least in part by out-of-country contractors, the organization needs to identify the relevant jurisdictions and assess the potential risks to the integrity, security and confidentiality of data when transferred to such a service provider.

Currently, Quebec's *Law 25* stipulates a requirement for a privacy impact assessment to be conducted for any out-of-province data transfer — addressing the sensitivity of the information, the purposes for which it will be used, the safeguards, including contractual safeguards, that will be applied, and the legal regime in the foreign jurisdiction, including the privacy principles applicable there. A similar requirement for a PIA, or as it is now referred to, a "transfer impact assessment," is provided for in the proposed PPCDA.

Ongoing monitoring and assessment: The organization should consider how ongoing monitoring and assessment of the performance and security of the provider's technology, including privacy compliance, can be performed. Considerations should include contractual provisions for maintaining access logs, reporting tools, regular testing and audits (both internal and external).

End of data life cycle: The organization should confirm the provider's procedures for destroying personal information at the end of its life cycle, including information stored on cloud servers, backups and information held by any subcontractors.

Contract termination: Finally, the contract should stipulate what happens to information once the provider's services are terminated, including how any personal information is transferred back to the organization, or another organization, and the procedures for deletion of any personal information not transferred back or transferred to a third party.

David Young is principal at David Young Law, a privacy and regulatory counsel practice in Toronto.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the author's firm, its clients, LexisNexis Canada, Law360 Canada or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Interested in writing for us? To learn more about how you can add your voice to Law360 Canada, contact Analysis Editor Richard Skinulis at Richard.Skinulis@lexisnexis.ca or call 437-828-6772.

All Content © 2003-2026, Law360 Canada