

OPC's guidance for contracting with service providers

The federal Office of the Privacy Commissioner has issued a draft guidance document addressing best practices for organizations contracting with third party service providers.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,¹ the guidance document 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 focusses 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 now-in force provisions of Quebec's Law 25 addressing privacy requirements for service provider relationships.² While both the current federal law, PIPEDA,³ 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So, while the draft guidance document talks in terms of assessing potential service providers, it can be understood as directed to fleshing out minimum recommended contractual provisions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.

Framed in the context of the current law, PIPEDA, the rationale for the guidance is explained as addressing compliance with PIPEDA's *Accountability Principle*.⁴ That principle states that organizations are responsible for personal information under their control, including personal information transferred to a third party for processing, and, as noted, 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

¹ [Guidance on assessing third-party service providers](#), Office of the Privacy Commissioner of Canada, September 10, 2026. The OPC is accepting comments on the draft document until December 4, 2026.

² *Act respecting the protection of personal information in the private sector*, s. 18.3.

³ *Personal Information Protection and Electronic Documents Act*.

⁴ Principle 4.1.3.

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.

Best practices check-list – contracting requirements

The guidance document sets forth a check-list of best practices that it recommends for inclusion in the assessment process. Key check-list items are set out below, with certain commentary added where relevant including with respect to contracting considerations.

Importantly, the OPC recommends that *a contract* set out the service provider's responsibilities in connection with providing the services and in particular its obligations for privacy compliance. To be noted, the OPC suggests including in the contract provisions addressing each of the assessment items identified in the check-list.

Identify the relevant personal information and where it will reside

The organization needs to identify and define the personal information that will be involved in the service provision. Knowing what personal information will be collected, used, or disclosed in the work product will assist the contracting organization identify the data that it will be responsible for under the law and the privacy risks involved. To assist in this process, it should map data flows and storage locations between the organization, its clients and any other individuals, the service provider, and any additional parties involved in providing the product or service such as sub-contractors. It should identify whether any of the personal information involved is sensitive personal information.

Where de-identified or anonymized data is involved, particular scrutiny should be included in the assessment and addressed in the contract. De-identified datasets may still contain personal information that could be re-identified. Particulars regarding the service provider's de-identification and anonymization protocols and safeguards against re-identification should be requested and minimum requirements set forth in the contract.

Set out the data use under the contract

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.

The assessment should confirm whether the provider's technology relies on the use of any training data, whether or not provided by the organization, to train an AI algorithm or test its functioning. In regard to any use of training data under the contract, the organization should request information about the source of the data and how the provider collected

it. The assessment should determine whether this sourcing is consistent with legal requirements under PIPEDA or other jurisdictions where it was collected.

Understand the functionality and performance of the provider's systems

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. It should ensure that, to the extent that any functionalities for data collection are not required or are outside the scope of the contract, they will be disabled.

The organization needs to understand how the provider's technology addresses known privacy risks in its functionalities such as systemic bias, security vulnerabilities, or factors potentially causing inaccuracies or discriminatory treatment. It should assess the measures that the provider has taken to reduce these risks and, if needed, obtain advice from expert consultants regarding mitigating the risks.

Assess and prescribe security practices and administrative controls

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.

The organization should understand the security features built into the design of the product or the technology being provided, including optional security settings that can be enabled or disabled, and confirm who is responsible for managing those settings.

Not noted in the draft guidance but a consideration for service provider relationships involving significant personal information processing, is whether the contracting organization should require the provider to be certified under a recognized security assessment framework such as SOC-2⁵ or to a recognized security standard such as ISO 27001.⁶

Address protocols for responding to 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.

The more extensive question to be addressed, not covered in the guidance document, will be the next steps, in terms of breach response and notifications, both internally and vis-à-vis external stakeholders including users of the product or service as well as regulators. A key issue will be delineating the respective functions of the organization and the

⁵ SOC 2 (or "Systems and Organization Controls 2") is an industry-recognized compliance framework that evaluates a service organization's security controls for personal data resulting in an attestation report issued by an accounting firm.

⁶ *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, ISO/IEC 27001:2002.

provider in the breach response protocol. The contract should include clear stipulations regarding the obligations and functions that the service provider will be required to perform, as well as procedures for communications and instructions between the organization and the provider in the responding to and resolving a breach situation.

Assess out-of-country data collection and 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. The OPC notes that organization's obligations in this regard remain governed by PIPEDA.

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. Only if the PIA "demonstrates that the personal information would be adequately protected, including with respect to generally accepted privacy principles" will the transfer be permitted.

A similar requirement for a PIA, or as it is now referred to, a "transfer impact assessment", is provided for in the proposed PPCDA.⁷ This provision stipulates that before disclosing or transferring personal information outside of Canada an organization must carry out, in accordance with the prescribed requirements, a TIA and implement measures to mitigate the risks identified in the TIA, such as contractual privacy protection measures, adherence to a code of practice or certification process approved by the regulator, or any other prescribed measures.

The OPC guidance clearly contemplates these current and anticipated requirements for organizations to assess the risks to data protection in foreign jurisdictions where the potential service provider operates. This "transfer impact assessment" will be a key item, and likely soon to be a statutory requirement, for addressing cross-border service provider relationships, to be identified not only as part of the assessment process but also in the resulting contract. That contract should include requirements for the service provider to assist in conducting the TIA as well as ensuring that compliance procedures stipulated be as a result of the TIA are implemented and continue to be evergreen.

Assess the risk of vendor lock-in and lock-out

The organization should assess the risk of becoming technologically dependent on a provider's proprietary technology or product. Such a "vendor lock-in" can limit the organization's control over processing of its data and can make it more difficult to switch providers in the event of unsatisfactory performance. The organization should consider contractual provisions for stipulating proprietary data formats and ensuring data portability. Consideration should be given to maintaining secondary data back-up facilities.

The organization also should assess the risk of the provider ceasing operations. A "vendor lock-out" can present serious issues regarding continuity of access to and recovery of data held by the provider. The organization should include in its

⁷ S. 57(1)

due diligence requirements information regarding the provider's history and supply-chain track record, as well as potential regulatory constraints relevant to its operations. As with the vendor lock-in risk, consideration should be given to maintaining secondary data back-up facilities.

Identify monitoring mechanisms

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

In particular, the organization should identify how the provider's compliance with its (i.e. the organization's) privacy obligations can be monitored, on an ongoing basis, for example through inspections or audits. The provider should identify how data is stored and retrieved for auditing purposes and for responding to individual access requests.

Confirm data retention and end of contract procedures

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

The organization should stipulate in the contract what happens to personal information held by the provider or any subcontractors once the provider's services are terminated, including how any personal information is transferred back to the organization and the procedures for deletion of any personal information not transferred back or transferred to a third party.

Conclusions

The OPC's draft guidance document addressing assessment of service providers is framed in the context of compliance with PIPEDA's Accountability Principle – that an organization that collects and processes personal information is responsible for the privacy protection and compliance respecting that information even when the information is held by a third-party service provider on behalf of the organization. However, in providing a useful check-list for conducting such an assessment for privacy purposes, the document in a broader frame will be useful for organizations in developing their service provider contracts, both in regard to privacy compliance items as well as more generally the overall contract performance considerations.

The OPC's check-list usefully serves both the due diligence and the contract drafting functions for establishing service provider relationships.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca
Note: The foregoing does not constitute legal advice. © David Young