大成 DENTONS

The ins and outs of transferring personal information to service providers

Organizations establish relationships with third-party service providers for many different reasons, for example, to optimize customer experience, enter into different markets and increase operational efficiencies. However, while business functions and services may be delegated to third parties, Canadian privacy regulators require an organization to remain accountable for the protection of personal information under any outsourcing arrangement.

In this article, we will examine how Canadian private sector privacy laws treat the transfer of personal information to service providers (in particular cross border transfers and the transfer to cloud service providers) and some practical business considerations to mitigate risk in this area.

The legislative landscape in brief – the accountability principle

The *Personal Information Protection and Electronic Documents Act*[1] (PIPEDA) is a federal law that applies to federal works, undertakings or businesses, and to provincially regulated businesses in provinces that do not have their own private-sector privacy law, for the collection, use and disclosure of personal information in the course of a commercial activity. Three Canadian provinces – Alberta,[2] British Columbia[3] and Québec[4] – have their own private-sector privacy laws that have been deemed to be "substantially similar" to PIPEDA. Where these laws overlap with PIPEDA, the provincial law applies.

PIPEDA sets out 10 principles for the collection, use and disclosure of personal information in the private sector.[5] Principle 1 is "accountability," which sets out that an organization is responsible for personal information under its control and must designate an individual or individuals who are accountable for the organization's compliance with the following principles (the Accountability Principle). According to the Office of the Privacy Commissioner of Canada (the OPC), an accountable organization must have in place policies and procedures which demonstrate, at a minimum, the capacity to comply with applicable privacy laws.[6] The Accountability Principle is implicit in Alberta, British Columbia and Québec's respective private-sector privacy laws.[7]

1 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

2 *Personal Information Protection Act*, S.A., c. P-6.5.

3 *Personal Information Protection Act*, S.B.C., c. 63.

4 *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 (Québec Act)

5 PIPEDA, Sch. 1.

6 Office of the Privacy Commissioner of Canada, et al., "Getting Accountability Right with a Privacy Management Program," April 2012..

7 Ibid.

The Accountability Principle is also found in the *Consumer Privacy Protection Act* (CPPA) the privacy law that has been advanced as part of Bill C-27 to replace PIPEDA. Under the CPPA the organization that is accountable for personal information is the one that collects it and determines the purpose for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself or by a service provider on behalf of the organization.[8]

Private sector organizations must protect personal information that is under its control, **including** information that has been transferred to a service provider.[9] Organizations are obliged to use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. According to the OPC, a "comparable level of protection" means that the service provider must provide protection that can be compared to the level of protection the personal information would receive if it had not been transferred.[10] Therefore, while the privacy protection measures that are adopted by service providers do not have to be identical, the OPC considers that they should be generally equivalent.[11]

When personal information is under an organization's possession or custody

The terms "control" or "custody" are not defined under PIPEDA. However, personal information in the custody of a service provider for the purpose of performing services on behalf of an organization, have been considered to be under the control of that organization where such organization retains the legal or contractual control of the information. The CPPA will go further by introducing a clear distinction between the controller and processor of personal information similar to the way in which those terms are used in the European Union's *General Data Protection Regulation*.[12]

The OPC's guidance on breach reporting says that it is reasonable to interpret the principal organization as having control of the personal information.[13] This assessment requires a case-by-case review of relevant contractual arrangements and commercial realities between organizations. Organizations must generally ensure that personal information in the hands of its service providers is adequately protected, as it may be ultimately responsible for any subsequent loss of or unauthorized access to or disclosure of personal information.

---

8 Bill C-27 "*An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*," Part 1, *Consumer Privacy Protection Act*, paragraph 7(2). Note that Bill C 27 completed its second reading on April 24, 2023.

9 PIPEDA, Sch. 1, clause 4.1.3.

10 Ibid.

11 Office of the Privacy Commissioner of Canada "Guidelines for processing personal data across borders", January 2009.

12 CPPA, paragraph 11(2).

13 "What you need to know about mandatory reporting of breaches of security safeguards." Revised: August 13, 2021. We note that the OPC, however, has said that determining who has personal information under its control needs to be assessed on a case-by-case basis.

Checklist of considerations – complying with the accountability principle

Review of existing service providers that have access to personal information	An audit of service providers and corresponding contractual agreements is necessary in order to map an organization's transfers of data. Organizations subject to PIPEDA (and similar provincial laws) are required to inform an individual, upon request, of the use and disclosure made of that individual's personal information, providing an account of the third parties to which it has been disclosed.[14] What personal information is involved, and who has access to it? A good understanding of this information will assist an organization in complying with its obligations under Principal 9 of PIPEDA and any potential future obligations under the CPPA.
Review or development of policies and procedures to establish a "Service Provider Management Program"	A Service Provider Management Program is important to have in place to ensure that an organization is handling personal information consistently and will be able to demonstrate its compliance with data privacy laws to its customers and to privacy regulators. The policies and procedures that are necessary for adequate protection of personal information depends on the scope and sensitivity of the personal information being handled, and the nature of the services being provided. These include limited access to personal information and ensuring that the appropriate security safeguards are in place.
Due diligence: Service providers' data management practices	Organizations should conduct due diligence to assess and mitigate any potential privacy risks before engaging a service provider that will handle personal information. As has been suggested by the OPC, risk assessment activities may include conducting an internal privacy impact assessment and obtaining legal advice on privacy and information security obligations both in Canada and, if applicable, in the foreign jurisdiction where the Service Provider operates.[15] An organization should approach any service provider relationship in the knowledge of what privacy laws process will include assessing whether the service provider's policies and processes align with its obligations under these laws.

14 PIPEDA, Sch. 1, cls. 4.9.1 and 4.9.3.

15 *Bank ensures openness and comparable protection for personal information transferred to third party*, 2020 CanLII 58761 (PCC) at para. 57.

Contractual arrangements with service providers	The primary means by which organizations can protect personal information in the custody of service providers is via contractual agreements. The OPC has found that contracts with service providers should include specific provisions regarding: • What personal information is being handled by the Service Provider; • What specific rules, regulations and standards need to be complied with in the handling of the information, including PIPEDA; • The roles and responsibilities of key stakeholders within both organizations for the handling of the personal information, including responsibilities for specific functions, decision-making, safeguards and breach response; • Information security obligations; • Acceptable uses of the information; • Retention and destruction obligations; and • Reporting and oversight arrangements, including written reporting obligations in the case of a breach that could compromise the personal information.[16] Consequences for non-compliance with contractual obligations including indemnity clauses and payments for all costs incurred including legal fees may also be considered. Agreements with service providers regarding the protection of personal information should also include specific requirements for employees of the service provider, and specific provisions to cover instances of subcontracting.[17]
Transparency	An organization is obliged under both PIPEDA and the CPPA to develop information to explain the organization's policies and procedures to give effect to the accountability principles described in this article. Provisions in an organization's privacy notice should be clear in this regard.

16 *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information*, 2019 CanLII 35618 (PCC) at para. 74.

17 *Bank customer objects to being surveyed by private firm*, 2002 CanLII 42306 (PCC).

Monitoring and enforcement

An organization must be able to confirm what happens to personal information after it is provided to a service provider. Thus, in addition to contractual guarantees regarding the protection of personal information, organizations should also put in place a structured program for monitoring and enforcement, which the OPC has found, may include:

- Mechanisms for periodic reporting by the Service Provider on the handling of the personal information;
- Mechanisms to ensure periodic external assessment (by the organization or an appropriate third party) of compliance with the obligations in the agreement;
- Requiring any issues identified during the course of any audit to be monitored by an independent auditor;
- Requiring the Service Provider to obtain sign-off by the independent auditor to confirm that all remedial actions have been effective; and
- Requiring the Service Provider to attest annually that it meets all contractual obligations.[18]

As mentioned, clause 4.1.3 under Schedule 1 of PIPEDA provides that organizations must use contractual or other means to provide a comparable level of protection while personal information is in the custody of a Service Provider. "Other means" may include non-contractual oversight and auditing mechanisms.[19] A discussion regarding whether a Service Provider holds any cyber insurance coverage may also be prudent in this case.

Jurisdictional considerations

Personal information is often transferred to service providers located in or who will store data in jurisdictions outside of Canada. PIPEDA does not prohibit the use of foreign Service Providers; however, organizations that transfer personal information to foreign-based service providers should notify individuals that the information may be available to the government of that country or its agencies under a lawful order made in that country.[20] More robust contracts may be required when a service provider is located in a foreign jurisdiction with a different privacy law regime.

18 We note that such measures were found to be satisfactory by the OPC (in light of other factors) *in Bank ensures openness and comparable protection for personal information transferred to third party*, 2020 CanLII 58761 (PCC) at para. 65.

19 Office of the Privacy Commissioner of Canada, "Interpretation Bulletin: Accountability" (April 2012).

20 Ibid.

Cloud service providers

The use of cloud services, which allow individuals and businesses to use software and hardware that are managed by third parties at remote locations, comes with various security and privacy considerations, including those considerations as referenced above. A transfer of personal information to cloud service providers is a common activity in today's landscape where digital transformation has been accelerated. As mentioned, PIPEDA does not prevent an organization from transferring personal information to an organization in another jurisdiction for processing, including the transfer of personal data to cloud service providers in other jurisdictions, however, it does set out certain rules governing those transfers.

Canadian privacy laws generally obligate organizations to support an information security program to protect the personal information that they collect and use, and to comply with any applicable sector-specific laws. Organizations are expected to adopt security measures that are reasonable in the circumstances and should protect personal information against loss, theft, or unauthorized access, disclosure, copying, use, or modification, according to its sensitivity. The OPC describes its view of reasonable data security practices in OPC: PIPEDA Self-Assessment Tool (July 2008).

It is important to understand where data may reside in order to fully understand the legal regimes for protecting personal information and the circumstances under which data may be accessed by foreign courts, government agencies and law enforcement. Some cloud providers offer customers some control over data residency and may set certain "availability zones," however, organizations will need to have an understanding of the relevant terms of service.

There are further restrictions to cross-jurisdictional personal data transfers in Alberta and Québec. The Alberta *Personal Information Protection Act* explicitly imposes obligations on organizations that use service providers outside of Canada to collect, use, disclose or store personal information. Organizations are obligated to notify individuals that they will be transferring individuals' personal information to a service provider outside the country, the purposes for which the service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization and to include information on outsourcing practices in the organization's policies. In Québec, privacy impact assessments must be conducted with respect to any transfer of personal information outside of the province and local counsel should be consulted with in light of recent changes to the Québec Act (as reported on here).

Organizations would be advised to consider the sensitivity of the information being transferred to a cloud service provider, the nature of the cloud computing deployment model and the terms of the contractual arrangement.

Summary

Given the trend in Canadian privacy legislation to increased regulatory authority and fines for non-compliance, businesses must address data privacy considerations (particularly from an accountability perspective) involved in all outsourcing arrangements. Organizations would be well advised to work through the checklist above to ensure that risk is mitigated in this area. Organizations may transfer the possession of its personal information to service providers, however, its legal and compliance obligations with respect to this information must remain top of mind.

If any questions arise regarding transferring personal information to service providers, you can reach out to the authors, **Kelly Osaka** and **Danielle Dudelzak**, or any member of the Dentons Canada Privacy and Cybersecurity team.

Contact

Kelly Osaka
Partner, Calgary
D +1 403 268 3017
kelly.osaka@dentons.com

Danielle Dudelzak
Associate, Calgary
D +1 403 268 6312
danielle.dudelzak@dentons.com

CSBrand-117522-Privacy Litigation Undone-Flyer-04 — 23/05/2023