Toronto Law Journal

Why Businesses of All Sizes in Canada Should Have Privacy Management Programs … If Not Now, Sooner Than Later

April Gougeon & Bill Hearn (with help from articling student Luciana Andrade)
Fogler Rubinoff LLP[1]

Since November 2020 and despite consensus that reform is necessary, Canada's federal government has struggled to find broad support for its proposed modernization of the country's 20-year old federal private sector privacy law — namely, the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**). The government's current attempt (Bill C-27, the *Digital Charter Implementation Act, 2022*), introduced in June 2022, languished in Second Reading until April 24th, 2023, when it was referred to the House of Commons Standing Committee on Industry, Science and Technology (also known as INDU). Earlier this month, Parliament continued to debate many foundational aspects of Bill C-27 including whether it should treat privacy as a fundamental or human right, include more enhanced protections for minors, and eliminate implied consent, to name a few.

That said, there seems to be a consensus amongst Canadian politicians and stakeholders (from industry to civil society) that every business subject to PIPEDA (and any modernized privacy law that replaces it) should have a comprehensive privacy management program (**PMP**) scaled to a number of factors including the size of the business and the volume and sensitivity of the personal information under its control. Perhaps this consensus is to be expected because PIPEDA's accountability principle (which obliges businesses to accept responsibility for personal information protection) has long required in Principle 4.1.4 that every business design and implement policies, procedures and practices to give effect to its obligations under PIPEDA.

PMPs under PIPEDA

In 2012, the Office of the Privacy Commissioner of Canada (**OPC**), and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia issued a seminal guidance document (that has stood the test of time) outlining their expectations for a comprehensive, robust, and effective PMP - *Getting Accountability Right with a Privacy Management Program* (**Guideline**). The Guideline describes in considerable detail what a business must do to implement and maintain a demonstrably credible PMP. The Guideline identifies many expectations of Canada's privacy commissioners but underscores that these expectations are not meant to provide businesses with a simple "one-size-fits-all" solution. Instead, when considering these expectations each business must take into account its particular situation and tailor its PMP to best operationalize its compliance with PIPEDA.

[1] Reprinted in the Toronto Law Journal with the permission of the authors

To this end, the Guideline recommends two building blocks for businesses to use when developing a compliant and effective PMP: specifically, each business should (1) take actions to develop an internal governance structure that cultivates a privacy-respectful culture and (2) create program controls to protect personal information under its control.

Regarding the first block, the Guideline states that a business should incorporate privacy protection into their internal data governance by taking at least the following actions:

- getting buy-in from senior management to champion the PMP;
- appointing someone (usually called the privacy officer) who is qualified and responsible for the PMP and giving them the powers and resources to implement the PMP;
- if necessary (e.g., in larger businesses), setting up a privacy office with staff to assist the privacy officer with their mandate; and
- establishing internal reporting mechanisms to help ensure that the PMP functions as expected.

Regarding the second block, the Guideline states that a business should implement at least the following PMP controls:

- establishing and maintaining a personal information inventory to determine all the personal information held by the business and to document why the business collects, uses or discloses that personal information, and how sensitive that personal information is;
- having internal privacy protection policies for employees to follow that help ensure the business meets its obligations under PIPEDA including policies regarding (a) the collection, use and disclosure of personal information, (b) access to and correction of personal information, (c) retention and disposal of personal information, (d) responsible use of information and information technology (including appropriate security and access controls), and (e) challenging compliance;
- establishing identification and mitigation processes and documents (including risk assessments) for privacy impacts and security threats;
- providing ongoing training on privacy protection policies and obligations to persons involved in handling personal information tailored to specific needs;
- creating protocols for privacy breach and incident management response that, among other things, assign responsibilities for privacy breach reporting;
- managing third party service providers to whom the business transfers personal information for processing by putting in place contractual or other means to protect that personal information (such as including specific provisions in a contract binding the service provider to the policies and protocols of the

business and requiring the service provider to notify the business in the event of a breach); and

- developing a procedure and approach to external communication for informing individuals of their privacy rights and the business's program controls in clear and understandable language.

The Guideline also outlines the following critical tasks involved in the ongoing assessment and revision of a business's PMP to ensure it remains relevant and effective including:

- developing an annual oversight and review plan with key performance measures and a schedule for review; and
- assessing (through regular monitoring and periodic audit) and where necessary revising program controls which requires the privacy officer to undertake at least the following actions:
    - monitor and update the personal information inventory;
    - review and revise privacy protection policies as needed to ensure they remain relevant and effective;
    - treat privacy impact assessments and security threat and risk assessments as evergreen documents;
    - review and modify training and education of employees;
    - review and adapt breach and incident management response protocols;
    - review and where necessary refine requirements in contracts with service providers; and
    - update and clarify external communication explaining privacy policies.

PMPs under Bill C-27

It seems reasonable to conclude that the PMP provisions in Bill C-27 are mainly a statutory codification of the Guideline. Notably, however, the Canadian privacy commissioners' expectations in the Guideline for all businesses in Canada to have a tailored PMP will be legally binding on businesses if the PMP requirements in sections 9 and 10 of the CPPA become law. Specifically, these provisions will:

- again, make it mandatory for businesses of all sizes in Canada to implement and maintain an appropriately scaled PMP;
- require the PMP to include the policies, practices, and procedures for the business to fulfill its privacy obligations; and
- in developing the PMP, require each business to take into account the volume and sensitivity of personal information under its control.

Moreover, the OPC will have the right, on request, to access the policies, practices and procedures of the business's PMP. While the OPC can provide guidance and corrective measures with regards to that PMP, the OPC cannot use the policies, practices and procedures it obtains through such access to initiate a complaint or carry out an audit.

More Guidance on PMPs

In addition to the Guideline, businesses can draw inspiration in establishing or updating their PMPs through the general guidance in the following recent publications:

- British Columbia's 2023 *Accountable Privacy Management in BC's Public Sector*;
- the International Organization for Standardization (**ISO**)'s 2023 *ISO/DIS 31700 Consumer protection — Privacy by design for consumer goods and services*; and
- the European Data Protection Board's 2020 *Guidelines 4/2019 on Article 25, Data Protection by Design and by Default*.

Why businesses should be proactive with their PMPs

For any business, compliant and effective privacy and data governance involves understanding its personal information flows, practices, risks, safeguards, procedures, and legal requirements. Having a comprehensive PMP is one of the best ways for a business to achieve and demonstrate accountability. It provides assurance to the business that it is both aware of its privacy obligations, as well as what personal information practices occur within its operations.

While the passage of Bill C-27 in its current form is not guaranteed, there has been little controversy about the PMP requirements proposed in the CPPA and likely for good reason. For the most part, these sections are a codification and evolution of the Guideline with which most businesses responsibly discharging their accountability obligations under PIPEDA have been familiar for many years.

Lastly, with the number and severity of cyber incidents on the rise and with Canada's federal private sector privacy law most likely soon moving from an ombuds model to an enforcement model with significant penalties and fines for non-compliance, prudence dictates that all Canadian businesses (whether large, medium or small) be proactive and, if they haven't already, now start the process of putting in place comprehensive, robust and effective PMPs appropriately tailored to their operations. Simply put, if a Canadian business takes the lead with a demonstrably credible PMP, it will be good for that business's customers, employees, service providers, relationship with Canadian privacy commissioners and, in turn, the business's bottom line and reputation.