Canada's Private-Sector Privacy Laws: Is Your Organization Compliant?

March 2025
By: Fiona Brown and Cathy Jares

The federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), along with certain provincial privacy laws, regulates how private-sector organizations manage personal information in commercial activities. Continue reading for an overview of what you need to know to stay compliant.

Which privacy laws apply to my organization?

PIPEDA regulates the collection, use and disclosure of personal information, including personal health information, in the course of conducting commercial activities.

- **Personal information** refers to any information about an identifiable individual, whether provided orally or in written/recorded form. This includes details such as name, address, age, ID numbers, employee files, ethnicity and social media comments. It does not include business contact information.
- **Commercial activity** includes any transaction, act or conduct of a commercial nature, such as selling, bartering or leasing donor, membership or other fundraising lists.

Non-profit organizations are not automatically exempt from PIPEDA. They may still engage in commercial activities unrelated to their non-profit mandate – even if, for tax purposes, they are considered not-for-profit organizations.

Certain provinces, including British Columbia, Alberta and Quebec, have enacted private-sector privacy laws that have been deemed substantially similar to PIPEDA. Businesses operating within such provinces are generally exempt from PIPEDA unless they engage in commercial activities that involve handling personal information across provincial and national borders or operate in federally regulated industries (such as telecommunications, banking, radio and television, etc.). Requirements under provincial privacy laws generally mirror those in PIPEDA.

Additionally, the provinces of Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have enacted legislation regulating the collection, use and disclosure of personal health information. This may include information about an individual's physical and mental health, health services received, and information collected incidentally during the provision of health services.

What are my obligations under PIPEDA?

All organizations subject to PIPEDA must abide by the Fair Information Principles and breach reporting obligations. Ultimately, the Privacy Commissioner's assessment of whether an organization is collecting, using or disclosing personal information in compliance with PIPEDA is context-dependent and requires an analysis of what is reasonable and appropriate in a specific circumstance.

Fair Information Principles

The following are key aspects of the Fair Information Principles:

- **Accountability:** Organizations must implement policies and practices to protect personal information and establish a process for complaints/inquiries (such as a Privacy Policy). They must also train employees and develop plain-language explanations of their policies and procedures for public disclosure.
- **Identifying Purposes:** Organizations should identify the purposes for which personal information is collected at or before the time of collection.
- **Limiting Collection:** Organizations must collect only the information necessary for the identified purposes.
- **Consent:** Organizations must obtain consent to collect, use and disclose personal information, except in instances where consent can be implied or where certain exemptions apply. Individuals must also be able to withdraw consent.
- **Safeguards:** Personal information must be protected by security safeguards appropriate to its sensitivity of the information.
- **Challenging Compliance:** Individuals must be able to challenge the organization's compliance using the organization's complaint procedures. Note that individuals can file a further complaint with the Privacy Commissioner against an organization for not following a recommendation or requirement under PIPEDA.

Reporting Obligations

Organizations must report a breach of security safeguards to the Privacy Commissioner if it is reasonable in the circumstances to believe that the breach creates "a real risk of significant harm" to an individual. This includes risks such as bodily harm, financial loss or identity theft. In such instances, organizations must also notify the affected individuals and relevant third parties. Furthermore, you must keep records of all breaches, even if they do not present a real risk of significant harm.

Next Steps

We're here to assist your organization with privacy law information and compliance, including:

- Identifying which privacy laws apply to your business.
- Auditing and assessing your current privacy practices and policies.
- Developing a written privacy policy, as well as other policies and procedures for your business.
- Implementing employee training plans.
- Responding to data breaches and determining whether a notification requirement has been triggered.

Have more questions about expanding into Canada? Please click here or scan the following QR code to access Aird & Berlis LLP's Market Expansion Dashboard, your one-stop-shop for market expansion resources:

AIRD BERLIS

Contact

Fiona Brown

Partner

T 416.865.3078

E fbrown@airdberlis.com

Fiona has extensive experience advising international businesses entering the Canadian market. To date, she has advised more than 100 companies expanding into Canada. Fiona advises clients in this space all day, every day. She has been practising for more than a decade and is a regular speaker and writer on market expansion matters. Fiona is proud to have been recognized by *The Best Lawyers in Canada, The Canadian Legal Lexpert Directory* and *Benchmark Canada*.

A proactive and comprehensive approach is required to succeed in a new market. Fiona manages teams of other lawyers and patent agents to provide her clients with a full range of legal services to help their businesses grow. She acts as project manager to ensure her clients receive seamless legal services in all relevant areas.

Fiona takes great care to understand her clients' businesses and deliver advice that is tailored to meeting their specific needs. Her responsiveness, dedication to clear communication and hands-on approach show that she is personally invested in the success of her clients.

Fiona is pleased to offer a multitude of resources answering often-asked questions about expanding into Canada, including this video and this one-page guide, all of which can be found on the Market Expansion Resources Dashboard.

Cathy Jares

Partner

Cathy is a member of the firm's Privacy & Data Security, Technology and Corporate/Commercial Groups. Her practice spans a wide range of corporate and commercial matters, including business formations, mergers and acquisitions, financing transactions and day-to-day advice on corporate governance matters. Cathy has in-depth experience working with clients in the technology sector, including startups and venture-backed companies. She assists them with raising capital and negotiating commercial arrangements, such as intellectual property licensing and development, procurement, consulting, and reseller and distribution agreements. Cathy also has expertise in the areas of data protection and privacy and frequently advises clients in various sectors on Canadian privacy law compliance and policy development.