Canadian privacy laws and data protection: PIPEDA and beyond

September 02, 2025

This article is part of a practical series written for international companies looking to establish, launch, operate or invest in a business Canada. Each article covers a major area of law in Canada — everything from employment laws to taxes. Access all the articles on the "Doing business in Canada: A practical guide from 'Eh' to 'Zed'" page.

Canada's data protection framework varies slightly depending on the province in which the entity operates, whether it is federally or provincially regulated, and whether it is handling personal information of customers and/or employees. Recent developments include substantial amendments to privacy legislation in Québec, some of which are already in force. Substantial reform to PIPEDA is currently being considered by Canadian parliament and is expected to be adopted within the next year. The Bill introducing this reform also proposes what would be Canada's first piece of legislation governing the development, use, and deployment of artificial intelligence. Finally, organizations transferring personal information outside Canada should keep in mind specific transparency requirements in this regard under Canadian law.

Personal information protection legislation

Canada's privacy laws and data protection laws include rules regarding both private-sector and public-sector privacy rights and responsibilities, as well as specific rules regarding personal health-related information.

Canada's privacy rules regarding protection of personal information may apply to organizations collecting information about Canadian residents even if the organization is not physically located in Canada.

Depending on the province(s) in which they operate, private-sector entities in Canada are subject to either federal or provincial legislation governing the collection, use and disclosure of "personal information". The purpose of the legislation is to balance individuals' privacy rights with the entity's need to obtain and use personal information for reasonable purposes. These laws also cover the retention, disposal and safeguards necessary to protect the confidentiality of personal information.

The federal PIPEDA applies to an entity if:

- it is a “federal work, undertaking or business” (*i.e*., the entity carries on business in a sector such as navigation and shipping, railways, inter-provincial transport, air transportation, communications, broadcasting and banking), in which case PIPEDA applies to all personal information it collects, uses or discloses, including information about its own employees; or
- it collects, uses or discloses personal information “in the course of commercial activities” and the province in which it is operating has not enacted a comprehensive personal information law recognized by the federal government as “substantially similar”;
- it transfers personal information, for consideration, out of the province in which it was collected.

The provinces of Québec (Act respecting the protection of personal information in the private sector, ARPPIPS), Alberta (*Personal Information Protection Act*, Alberta PIPA) and British Columbia (Personal Information Protection Act, BC PIPA) have all enacted personal information legislation that has been recognized as “substantially similar” to PIPEDA. Accordingly, PIPEDA does not apply to the collection, use or disclosure of personal information in those provinces, although it does continue to apply to inter-provincial or international transactions involving personal information, and to federal works, undertakings and businesses in those provinces.

Under all these statutes, “personal information” is broadly defined, generally as “information about an identifiable individual”, with a few exclusions. For example, PIPEDA does not apply to personal information used to communicate with an individual relating to his or her employment or business such as the individual’s name, title, work, work address, telephone number, work fax number or work electronic address, that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to his or her employment, business or profession. The Alberta PIPA and BC PIPA include similar provisions, and the BC PIPA excludes “work product” of employees from the definition of “personal information”. In Québec, recent amendments to ARPPIPS exclude “personal information concerning the performance of duties within an organization by the person concerned” from the scope of its notice and consent requirements.

Importantly, an entity falling within category (2) above (*i.e*., a provincially regulated entity) is not subject to PIPEDA with respect to information about its own employees. This is because, under the Constitution, the federal government lacks jurisdiction to legislate on employment relationships that are governed by provincial law. However, the province’s personal information legislation in Québec, Alberta and British Columbia does apply to employee information.

All provinces other than British Columbia have also enacted legislation specifically governing the collection and disclosure of “personal health information”. Some, but not all, of that legislation has been recognized as “substantially similar” to PIPEDA for limited purposes. While such legislation applies primarily to practitioners and organizations in the health care sector (such as doctors and hospitals), it can also apply to an employer that has personal information about an employee (for example, in connection with a disability or the employee’s return to work after an accident or illness). Québec is the most recent province to have enacted legislation in respect of personal health information; Bill 3 “An Act respecting health and social services information and

amending various legislative provisions" was adopted in April 2023 and will come into force upon governmental decree.

PIPEDA and its provincial counterparts generally require compliance with the following principles:

- Accountability: An organization is responsible for personal information under its control and must designate an individual or individuals who are accountable for its compliance with the legislation. Unlike the "data protection officer" under the GDPR, the individual exercising this role under Canadian law does not have to be independent.
- Identifying Purposes: The purposes for which personal information is collected must be identified by the organization at or before the time the information is collected.
- Consent: The knowledge and consent of the individual are generally required for the collection, use or disclosure of his or her personal information, unless an exception applies. Consent may be express or implied, depending upon the circumstances and the type of information. The federal OPC, the Alberta OIPC and the BC OIPC have recently published Guidelines for obtaining meaningful consent, which will come into force in January 2019.
- Limiting Collection: The collection of personal information must be limited to what is necessary for the purposes identified by the collecting organization.
- Limiting Use, Disclosure and Retention: Personal information must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only so long as necessary to fulfill those purposes.
- Accuracy: Personal information must be as accurate, complete and up to date as is necessary for the purposes for which it is to be used.
- Safeguarding: Personal information must be protected by security safeguards appropriate to the sensitivity of the information (i.e., physical, organizational and technological measures). The notion of sensitive information has been the subject of an interpretation bulletin by the OPC.
- Openness: An organization must make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- Individual Access: On request, an individual must be informed of the existence, use and disclosure of his or her personal information and must be given access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended, as appropriate.
- Challenging Compliance: Individuals must be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Of particular note, if a Canadian transfers personal information outside Canada (*e.g.*, to an international parent company or service provider outside Canada), the Canadian organization is expected to disclose those facts in its privacy policy in order to meet its obligations under the openness and safeguarding principles. While this has been held to be an implicit requirement in privacy legislation across Canada, it is made explicit in the Alberta PIPA. In Québec, the amended ARPPIPS contains similar explicit transparency requirements, and further restricts transfers of personal information outside the province by requiring that the destination jurisdiction provide "adequate protection," ascertained

by a privacy impact assessment. The assessment must consider factors such as the sensitivity of the information, the purposes of its use, relevant safeguards, and legal regimes applicable in the destination jurisdiction. Organizations must also have a contract in place with the foreign service provider detailing the security measures the service provider must have in place to ensure a comparable level of protection to the personal information of Canadians.

PIPEDA, the Alberta PIPA, and Québec's ARPPIPS all impose specific breach notification obligations on organizations when there is a risk of serious or significant harm/injury. PIPEDA and Québec's ARPPIPS also require that a detailed and up-to-date register of breaches be maintained internally within an organisation. In British Columbia the privacy regulator recommends that organizations report breaches to the regulator and notify affected individuals.

Other privacy obligations

In addition to PIPEDA and provincial legislation dealing specifically with the collection, use and disclosure of personal information in the private sector, businesses may have additional statutory privacy obligations. For example, several provinces have enacted legislation that makes it an actionable wrong for one person, wilfully and without claim of right, to violate another's privacy. British Columbia Privacy Act is an example of such legislation. Under the B.C. Privacy Act, the nature and degree of privacy to which a person is entitled in any situation will depend on what is reasonable in the circumstances, giving due regard to: the lawful interests of others; the nature, incidence and occasion of the act or conduct; and any relationship between the parties.

Québec's Civil Code, the Québec Charter of human rights and freedoms and the Québec Act to establish a legal framework for information technology provide additional privacy obligations, including a statutory tort for privacy violations. In Ontario, the privacy tort of intrusion upon seclusion was recognized in 2012.

Businesses dealing with Canadian governmental bodies should also be aware of the privacy aspects of federal and provincial access to information legislation, such as the provincial freedom of information and protection of privacy statutes, the federal *Access to Information Act* and the federal Privacy Act. Subject to certain exceptions, these statutes generally restrict the ability of governmental bodies to disclose personal information to third parties, and in British Columbia, impose obligations on private-sector businesses that act as "service providers" to governmental bodies. These statutes also impose significant obligations on governmental bodies that do not exist for private enterprises, and ought to be considered when disclosing information to them.

Canada's Anti-Spam Legislation (CASL)

CASL is a very stringent law that regulates more than spam. It applies to commercial electronic messages sent to customers and business partners and requires express consent from the recipients for the sending of such messages, except in specific and limited situations where consent is deemed to be implied. Contravention of CASL is subject to significant fines.

Canada's federal anti-spam legislation, which came into force in 2014, sets out a comprehensive set of rules that govern the sending of electronic messages in Canada or to recipients in Canada. It is likely the strictest and most comprehensive law addressing electronic communications in the world. Note that Canada also has adopted the Unsolicited Telemarketing Rules, which apply to telemarketing.

CASL prohibits sending commercial electronic messages (which includes emails and text messages) unless consent has been obtained from the recipient. CASL also requires certain prescribed content and an "unsubscribe" mechanism to be included in the message. Despite its name, the law goes well beyond spam communications, covering electronic messages to customers and between companies sent from or accessed from devices located in Canada. The law also contains provisions dealing with altering transmissions data in electronic messages and preventing the installation of computer programs on another person's computer in the course of a commercial activity, without the person's knowledge and consent. Unlike the U.S. law, which requires that consumers receive an opt-out option, CASL requires opt-in consent for the sending of an electronic messages for a commercial purpose (which is defined broadly), except in specific and limited situations where consent is deemed to be implied (for instance where there is an "existing business relationship").

Those who violate the rules can face substantial fines. There is a maximum of C$1 million per violation in the case of an individual and up to C$10 million per violation for organizations. Although the private right of action has recently been suspended, CASL contraventions remain subject to regulatory enforcement, which can involve time-consuming and costly regulatory investigations and enforcement proceedings. So far, there have been fines of up to C$200,000.

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749