



# 12.

---

## Privacy Laws

### Overview

Privacy in Canada is governed by a collection of public sector, private sector, and health sector privacy laws (and by a related regime in Canada's anti-spam legislation (CASL) which is addressed in the Technology chapter of Doing Business in Canada). Depending on the sector, these laws exist at the federal and/or provincial level and may be supplemented by common law considerations. This chapter focuses primarily on Canada's federal private sector statute given its broad application to Canadian businesses.





## Private Sector

### PIPEDA

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada's federal private sector law that governs the collection, use, and disclosure of personal information.

### Defining Personal Information

Personal information is broadly defined in PIPEDA as "information about an identifiable individual." Such information can include, among other things, a person's name, address, phone number, age, sex, ethnicity, religion, education, and health and financial information. Certain government-provided information is also considered personal, such as a person's social insurance number, provincial health insurance plan number, driver's licence number, and passport number.

PIPEDA excludes business contact information from the application of the law where it is collected, used, or disclosed solely to communicate with an individual in relation to their employment, business, or profession.

### Application of PIPEDA

In general terms, PIPEDA applies to an organization's collection, use, or disclosure of personal information in the course of commercial activities, including:


- Provincially regulated organizations in respect of their collection, use and disclosure of personal information within provinces that do not have privacy laws that are substantially similar to PIPEDA (Alberta, British Columbia, and Québec have their own private sector privacy laws that have been deemed substantially similar to PIPEDA).

- Organizations transferring personal information across national or provincial borders.

PIPEDA also applies to the personal information of employees when it is collected, used, or disclosed in connection with the operation of a federal work, undertaking, or business (such as banks, airlines or other inter-provincial or international transportation, telecommunications companies, offshore drilling operations, and radio and television broadcasting).

PIPEDA does not apply to the collection, use, or disclosure of employees' personal information where individuals are employees of organizations under provincial jurisdiction (i.e., organizations that are not federal works, undertakings, or businesses). As noted, PIPEDA does not apply to provincially regulated organizations' collection, use or disclosure of personal information within British Columbia, Alberta or Québec. The general principles of PIPEDA are:

- Accountability
- Identifying purposes
- Consent
- Limiting collection
- Limiting use, disclosure, and retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance



## PIPEDA and Your Business

### Knowledge and Consent

Informed consent is the guiding principle behind PIPEDA. At or before the time of collection, individuals should be made aware of the purposes for the collection, use, or disclosure of their personal information, and they should have the right to grant or withhold their consent. Consent is valid only if it is reasonable to expect that the affected individual would understand the “nature, purpose, and consequences” of the collection, use, or disclosure of the personal information to which they are granting access.

There are certain exceptions to the consent requirement. For example, there is a consent exemption available for information collection where such collection is for the benefit of the individual in question and consent cannot be obtained in a timely way or where the information is “publicly available”, the scope of which is narrowly prescribed by the regulation. Individuals can provide consent in a variety of ways, including expressly, impliedly, or through an opt-out mechanism.

The appropriate form of consent that an organization must obtain will depend on the sensitivity of the personal information involved and on the individual’s reasonable expectations given the circumstances.


### Business Transactions

It is often necessary for organizations to collect, use, or disclose personal information, including employees’ personal information, in relation to due diligence and closing a business transaction.

PIPEDA permits these activities without consent, provided that:

- The organization has entered into an agreement that requires the recipient to (a) use the information for the sole purpose of the transaction, (b) protect the information, or (c) return or destroy the information if the transaction does not proceed.
- The personal information is necessary to determine whether or not to proceed with the transaction and, if a decision is made to proceed, to complete the transaction.
- For completed transactions, the organization must enter into an agreement that requires it to (a) use and disclose the information for the sole purposes for which it was collected, used, or disclosed prior to the transaction; (b) protect the information; and (c) give effect to any withdrawal of consent.
- The information must be necessary for carrying on the activity that was the object of the transaction, and one of the parties must notify the individuals within a reasonable time of the transaction and disclosure.

The above exemption does not apply if the transaction is for the primary purpose of purchasing (or otherwise acquiring), selling, disposing or leasing of personal information. The exemption codifies common practice and is modelled on similar provisions in provincial privacy laws in British Columbia and Alberta.



## **Outsourcing of Data Processing to the United States**

Canadian corporations may outsource certain data processing activities to a US parent corporation or a third-party processing company located within the United States or another jurisdiction. Although PIPEDA does not prohibit the outsourcing of data processing activities, it does make the Canadian organization accountable for the personal information while it is transferred to a third party for processing on the organization's behalf.

In addition, the Canadian organization will have to comply with two requirements imposed by the Office of the Privacy Commissioner of Canada (the "Commissioner"). First, as with all third-party processing (whether it takes place within or outside of Canada), the organization must protect the confidentiality and security of the personal information either by implementing adequate contractual and other safeguards between the organization and the other entity or through ensuring that those entities are governed by the same privacy policy that imposes the same privacy requirements on both entities. Second, the disclosing entity in Canada must notify the affected individuals if their personal information will be stored, used, or disclosed in a jurisdiction outside of Canada and that the information may be accessible under the laws of the relevant jurisdiction.

In addition to the above requirements, the Commissioner expects Canadian organizations to conduct due diligence on the legal requirements in the jurisdiction where the third party operates, including "potential foreign political, economic and social conditions" that may undermine its ability to properly safeguard personal information in advance of any transfer. The Commissioner also expects organizations to engage in appropriate monitoring, oversight and enforcement of the contractual and other safeguards noted above.

Additional requirements may be applicable in respect of certain types of information and pursuant to provincial privacy laws.

## **Breach Notification and Record Keeping**

Unless otherwise prohibited by law, PIPEDA requires organizations to notify individuals about, and to report to the Commissioner, all breaches where it is reasonable to believe that the breach creates a "real risk of significant harm to an individual."

PIPEDA defines "significant harm" as including, among other harms, humiliation, damage to an individual's reputation or relationships, and identity theft. A "real risk" requires consideration of the sensitivity of the information, the probability of misuse, and any other prescribed factor.

The notice to individuals and the report to the Commissioner must be given in the prescribed form "as soon as is feasible" after it is determined that a breach occurred. The Commissioner may publish information about such notices if it determines that it would be in the public interest to do so.

Pursuant to the Breach of Security Safeguards Regulations under PIPEDA, the notice to an individual must contain certain information, including a description of (a) the circumstances of the breach, (b) the personal information that is the subject of the breach, (c) the steps taken by the organization to reduce the harm that could result, and (d) the steps the individual can take to reduce or mitigate the harm. The notice must be conspicuous and given directly to the individual except in certain circumstances where indirect notice (e.g., posting to a website) may be permitted.



The report to the Commissioner must contain certain information, including the number of individuals affected, contact information for someone who can answer the Commissioner's questions, and a description of (a) the circumstances of the breach, (b) the personal information that is the subject of the breach, (c) the steps taken by the organization to reduce the harm that could result, and (d) the steps the organization has taken to notify the affected individuals. The report may be sent by "any secure means of communication" and may be updated with new information as the organization becomes aware of it.

Where notice is given to individuals, Section 10.2 of PIPEDA requires organizations to notify other organizations (e.g., credit bureaus) and government agencies if such notice could reduce the risks or mitigate the harm. Consent is not required for such disclosures.

In addition to the above notification and reporting requirements, PIPEDA requires organizations to keep and maintain a record of every breach of safeguards involving personal information under their control. Pursuant to Section 6 of the *Breach of Security Safeguards Regulations*, these records must be maintained for 24 months after the day on which the organization determines the breach happened. The records must also contain the information necessary to allow the Commissioner to verify compliance with the above reporting and notification requirements.

In addition, upon request, organizations must provide the Commissioner with such records. The Commissioner may publish information from such records if it would be in the public interest.


It is important to note that there is no threshold associated with the record-keeping obligation; a record of all breaches of security safeguards must be kept, irrespective of whether or not they gave rise to a real risk of significant harm. Nor is there any threshold before an organization would be required to provide its "breach file" to the Commissioner.

### Provincial Legislation

The provinces of Québec, Alberta, and British Columbia have enacted privacy legislation that is substantially similar to PIPEDA. As a result, the provincial legislation will apply to the collection, use, or disclosure of personal information within those jurisdictions (though PIPEDA will continue to apply to inter-provincial and international transfers of personal information and to employees of federally regulated organizations).

In Québec, the *Act to modernize legislative provisions as regards the protection of personal information* has fully come into force as of September 2024. Commonly referred to as Law 25, this Act has brought significant changes to Québec's private sector and public sector privacy laws, amongst others. Law 25 notably requires companies in Québec to:

- Designate a privacy officer to oversee the application of privacy laws (this role will be attributed to the company's highest authority in the absence of a written delegation to someone else)
- Notify the Commission d'accès à l'information and affected individuals in case of privacy breaches that meet a certain severity threshold ("serious risk of injury")

- 
- Perform Privacy Impact Assessments in a variety of situations, including before processing certain personal information in the context of technological projects or before disclosing personal information outside of Québec
  - Allow the affected individuals to exercise new rights, including a data portability and a re-indexation right
  - In case of non-compliance, pay fines up to a maximum amount of CAD \$25,000,000, or an amount corresponding to four per cent of worldwide turnover for the preceding fiscal year (whichever is greater).

Businesses operating in Québec should be mindful of these provisions.

### **Public Sector**

Federal, provincial, and territorial statutes regulate the collection, use, and disclosure of personal information by public bodies. Additionally, the Canadian Charter of Rights and Freedoms (the “Charter”) protects certain privacy interests (for example, section 8 of the Charter protects “personal, territorial and informational” privacy through the right to be free from unreasonable search and seizure by the government). The Criminal Code also provides some privacy protections, such as the offense of voyeurism and publication of intimate images.

### **Health Sector**

Most provinces and territories have their own health privacy legislation. Health privacy legislation applies to healthcare providers, as well as their service providers and agents. In addition to that legislation, regulators of health professions will also impose requirements regarding patient confidentiality.


### **Modernization of Canada’s Privacy Laws**

With the more common reliance on and the advancement of technologies having an impact on privacy protection, such as cloud computing and artificial intelligence, privacy protection became a public concern in the recent years and is now under scrutiny. As a result, notably in order to strengthen the protection of personal information, Canadian federal and provincial governments are modernizing their privacy laws.

At a federal level, on June 16, 2022, the Canadian federal government introduced Bill C-27, the *Digital Charter Implementation Act*, which would replace the PIPEDA privacy protection framework with the Consumer Privacy Protection Act.

Bill C-27 keeps the well-established consent-based regime of PIPEDA whereby companies are required to obtain the consent of the individual for collection, use, and disclosure of personal information. However, it provides flexibility for companies by (a) introducing two new exceptions to consent for “legitimate interest” and “business activities” that could be relied on by companies to the extent that the processing of personal information is not for the purposes of influencing an individual behavior or decisions; and (b) enabling transfers to service providers without consent of the individuals if personal information is used for the purposes of which it was transferred and adequate safeguards are in place.

Bill C-27 also addresses the need for Canadian privacy laws to evolve with new technologies as it introduces different definitions and associated protections for de-identified information and anonymized information, and a new proposed *Artificial Intelligence and Data Act*, which regulates “artificial intelligence systems” and the processing of data in connection with artificial intelligence systems.



Additionally, and importantly for businesses, Bill C-27 creates a more stringent environment for companies processing personal information by adding enhanced and expanded enforcement tools and severe remedies in case of non-compliance, such as:

- The ability for the Commissioner to recommend, and for the newly created Personal Information and Data Protection Tribunal to impose, penalties up to the greater of \$10 million or 3% of an organization's annual global revenues
- Significantly expanded offences with fines up to the greater of \$25 million or 5% of annual global revenues
- A private right of action to permit recourse to the courts in certain circumstances

These changes contemplated by Bill C-27 are consistent with the global trend towards the strengthening of privacy rules initiated by the European Union (GDPR), and changes brought at a provincial level in Québec.

In Québec, the *Act to modernize legislative provisions as regards the protection of personal information* has fully come into force as of September 2024. Commonly referred to as Law 25, this Act has brought significant changes to Québec's private sector and public sector privacy laws, amongst others. Law 25 notably requires companies in Québec to:

- Designate a privacy officer to oversee the application of privacy laws (this role will be attributed to the company's highest authority in the absence of a written delegation to someone else)
- Notify the Commission d'accès à l'information and affected individuals in case of privacy breaches that meet a certain severity threshold ("serious risk of injury")

- Perform Privacy Impact Assessments in a variety of situations, including before processing certain personal information in the context of technological projects or before disclosing personal information outside of Québec
- Allow the affected individuals to exercise new rights, including a data portability and a re-indexation right
- In case of non-compliance, pay fines up to a maximum amount of CAD \$25,000,000, or an amount corresponding to four per cent of worldwide turnover for the preceding fiscal year (whichever is greater)

Businesses operating in Québec should be mindful of these provisions.

### **CASL – the Anti-Spam Law**

Sending commercial electronic messages (CEMs) to and from electronic addresses in Canada and installing computer programs on systems in Canada is primarily governed by a statute commonly known as Canada's Anti-Spam Law (CASL) and the regulations made pursuant to it. There is overlap between the activities regulated by CASL and under PIPEDA, such that both laws must be considered. For a discussion of the requirements of CASL, please see the Technology chapter of Doing Business in Canada.

---