

Canadian data privacy laws: What's new, what's next

Canadian data privacy law sets the rules for how organizations collect, use, and protect personal information. Learn your rights and compliance steps



By [Kairos Anggadol](#)

Oct 10, 2025

Share

Contents

1. [What are the Canadian data privacy laws?](#)
2. [PIPEDA](#)
3. [Privacy Act](#)
4. [CPPA](#)
5. [Provincial data privacy laws](#)
6. [How can lawyers help clients with data privacy laws?](#)
7. [Canadian data privacy laws: timely protections in the digital age](#)

Canadian data privacy laws do not just protect personal information but also affect how businesses manage information they gather and handle. In this article, we will discuss the different data privacy laws in Canada and how they affect you and your business. If you have questions about compliance or privacy law, consulting a data privacy lawyer can help you understand your obligations and reduce legal risks.

What are the Canadian data privacy laws?

Canadian data privacy laws set the rules for how personal information is collected, used, stored, and protected by government and private sector organizations. These laws help keep people's personal details safe and give individuals important rights over their own information.

Laws on data privacy fall under the jurisdiction of both the federal and provincial governments. Both levels of government have laws that govern different aspects of protecting personal information.

Recent Articles



[Canadian Investment Regulatory Organization to invest \\$1.55m in not-for-profits](#)



[In-house professionals who don't use genAI tools cite distrust of reliability, quality: survey](#)



[LCM Attorneys: A litigation powerhouse for today's complex business environment](#)

Here's a summary of the main Canadian data privacy laws:

- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Privacy Act
- Consumer Privacy Protection Act (CPPA)

“Canada’s data privacy law landscape is like a mosaic – there are privacy laws from varying levels of government that apply to different aspects of society,” says Imtiaz Karamat, associate lawyer of [Deeth Williams Wall LLP](#). “For example, there are privacy laws for government bodies, private organizations, and specific industries.”

Karamat says that in his practice, they commonly focus on the federal PIPEDA, which applies to many Ontario businesses. “We also work with the Personal Health Information Protection Act (PHIPA), which is Ontario law for the health sector.”

We’ll discuss these laws below; you can also use the table of contents above to browse through these laws.

PIPEDA

As the main Canadian data privacy law, the [PIPEDA](#) governs the collection, use, handling, and disclosure of personal information during the commercial activities of:

- private organizations
- federally regulated organizations

“PIPEDA may apply to a private organization’s collection, use, disclosure, and handling of personal information when carrying out commercial activities,” says Karamat, who is also a certified Information Privacy Professional. “It includes privacy practice requirements for organizations to meet during their regular operations. It also requires organizations to take steps in specific circumstances, such as the reporting of data breaches to Canada’s Privacy Commissioner.”

In enforcing the PIPEDA, organizations are guided by the law’s ten principles. Watch this video to learn about these principles:

All you Need to Know about the 10 Canada PIPEDA Principl...



Got questions about Canadian data privacy laws? Consult the [best data privacy and cybersecurity lawyers in Canada](#) as ranked by Lexpert.

“Personal information”

The PIPEDA has a wide definition of what “personal information” is. It means all information “about an identifiable individual,” including a person's:

- ID numbers
- financial information (e.g., salaries, wages, credit or banking records)
- employment history
- ethnic or Indigenous origin
- medical records (e.g., blood type, medical history)
- personal views and opinions
- digital footprints (e.g., sites you visited, information given to websites)
- usual information such as name, age, address, sex, and gender

“Commercial activity”

If an organization is not engaged in a commercial activity, the PIPEDA will not apply to that organization. Under the PIPEDA, commercial activities include:

- any regular course of conduct that is commercial in character
- the selling, bartering, or leasing of donors, membership, or other fundraising lists

“Valid consent”

The PIPEDA states that consent is valid only if an individual is reasonably expected to understand why their personal details are being collected. This includes understanding the consequences for any breach or violation of the law.

Protections under PIPEDA

The collection, use, and disclosure of personal data must be with the express and valid consent of the person whose information is being collected. Related to this are the following rules:

- **organization's accountability:**
 - organizations are responsible for their storage and protection against violations by third parties
 - organizations may designate an individual to be accountable for their compliance with PIPEDA
- **according to purpose:** the collection, use, and disclosure of personal data must be for the appropriate purposes of that organization and those an individual may reasonably expect in each circumstance
- **disclosure to individuals:** organizations must exert all efforts to inform individuals:
 - what information will be collected
 - how it will be stored and used

- whether it will be passed on to third parties
- for what purpose it is collected and passed

Exceptions to the consent requirement

However, there are instances where consent is not required under the PIPEDA:

- if required by law (e.g., other statutes)
- if the collection and use either:
 - are in the interests of the individual, but their consent cannot be obtained in a timely manner
 - would compromise the information's availability or accuracy, and the collection is related to a breach of an agreement or a violation of a law
- if the disclosure is either:
 - required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records
 - made to another organization to investigate a breach of an agreement or a violation of a law, and the disclosure would compromise the investigation
 - made to another organization to detect, prevent, or suppress fraud, and the disclosure would compromise these actions against fraud

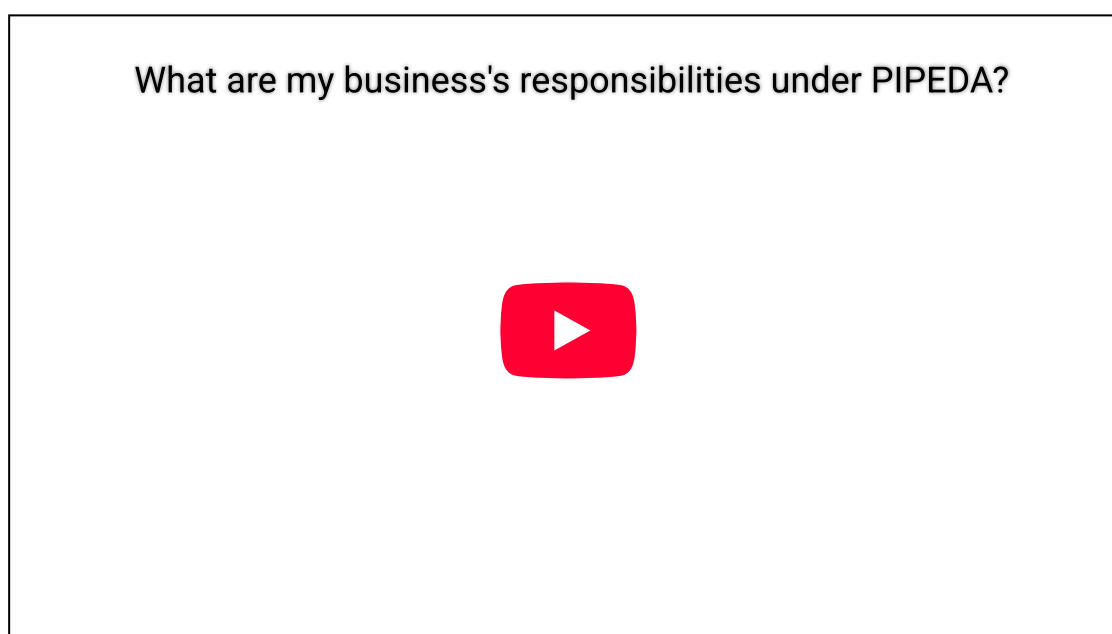
Breaches and complaints

When there is a data breach or [breach of privacy](#) under the control of an organization, it should:

- report the breach to the Office of the Privacy Commissioner
- notify the affected individuals

The PIPEDA grants remedies to individuals whose rights may have been violated, such as the filing of a complaint before the Privacy Commissioner. This will then trigger an investigation into the complaint. If the investigation has been discontinued, the complainant may apply to the court for a hearing.

If you're a business owner, you can watch this video to know more about your responsibilities under the PIPEDA:



Wondering how Canadian data privacy laws will affect you or your business? Talk to these *Lexpert*-ranked [best law firms for data privacy and cybersecurity in Canada](#).

Privacy Act

The [Privacy Act](#) applies to the personal information collected and stored by the government:

- from private individuals
- from federal employees through government institutions

Some examples of activities done by the government, to which the Privacy Act applies, are:

- border control and protection
- employment insurance
- enforcement of national laws
- old age security benefits
- tax processing and reimbursements

Restrictions on data privacy

Under this law, personal data may only be collected by the government when it is related to its programs. As a rule, it cannot be disclosed without the consent of the individual, unless it is:

- for the purposes for which it was collected
- authorized by a federal law
- in compliance with subpoenas, warrants, or orders of a court
- beneficial to the individual
- public interest outweighs the invasion of privacy

Also, government agencies are required to:

- ensure that the personal information it uses is accurate, up to date, and complete
- retain the information it collects for up to two years, unless the individual consents to its disposal

Investigations for violations

The Act has also established a person's right to access their information upon their request. When any of these rights have been violated, the Privacy Commissioner can receive and investigate these complaints.

These may include allegations:

- that an individual's personal information was used or disclosed without their consent
- when the individual has been refused access to their personal data

CPPA

[Bill C-27](#), also called the Digital Charter Implementation Act, 2022, was proposed to amend the PIPEDA. The CPPA was part of Bill C-27.

However, Bill C-27 died when Parliament was prorogued in 2025. This means that unless CPPA is refiled and passed as a law in the future, the current form of the PIPEDA stands as the federal Canadian data privacy law.

Provincial data privacy laws

Each province and territory either has its own laws on data privacy for the private sector or simply adopt the federal rules. Health information often gets some special protection at the provincial level.

Here's an overview of the main privacy laws across Canada:

- **Personal Information Protection Act (PIPA):**
 - covers private-sector organizations and works like PIPEDA, such as the rules for collecting, using, and sharing personal information in business
 - Alberta and British Columbia both have their own PIPA
- **Act Respecting the Protection of Personal Information in the Private Sector:**
 - covers private-sector organizations in Québec and works as PIPEDA
 - recent changes under Bill 64 (Law 25) made this law stricter, with new rules for consent, breach notification, and fines
- **Personal Health Information Protection Act (PHIPA):**
 - applies to health information custodians in the province, and gives patients different rights when it comes to their health information

- enacted in Ontario, but similar laws also exist in New Brunswick, Newfoundland and Labrador, and Nova Scotia

As an example of a provincial data privacy law, Karamat gave some of the highlights of the PHIPA. “PHIPA governs the collection, use, disclosure, and handling of personal health information.”

Like PIPEDA, Karamat says, PHIPA requires regulated entities to comply with certain privacy practices during their regular operations and in specific circumstances, such as notifying the Information and Privacy Commissioner of Ontario if personal health information is lost, stolen, used, or disclosed without authority.

“Notably, PHIPA allows the Information and Privacy Commissioner of Ontario to issue administrative penalties, which they used for the first time in August 2025,” he adds.

This case involved a doctor and a private clinic who violated the PHIPA, which issued fines against the two.

How can lawyers help clients with data privacy laws?

There are a lot of ways that [data privacy lawyers](#) can assist businesses that collect or handle this data, or the individuals whose information has been collected:

- guide businesses to comply with applicable laws
- help businesses create internal privacy policies
- guide individuals in filing complaints in case of a data breach
- represent clients in investigations, or in court if needed

“Privacy lawyers help clarify Canada’s legal landscape for clients to take the necessary steps to ensure their business’ success,” Karamat says. “This includes advising clients on maintaining a proper privacy posture for their regular operations and supporting them during any unique challenges that may arise from time to time.

“Our data privacy landscape is constantly evolving in response to risks associated with new technology and privacy lawyers help their clients keep pace with these changes.”

Canadian data privacy laws: timely protections in the digital age

Understanding Canadian data privacy laws helps businesses and individuals make better choices about how information is handled. But as these laws continue to develop to adjust to new technologies and risks, businesses must pay attention to these changes to prepare and avoid penalties. In these situations, data privacy lawyers are available to provide legal advice when needed.

Subscribe to the free [Lexpert newsletter](#) for your daily legal FAQs, including more articles on Canadian data privacy laws.

[PRIVACY](#) | [COOKIE POLICY](#) | [CONSENT PREFERENCES](#) | [TERMS OF USE](#) | [TERMS & CONDITIONS](#)
[ABOUT US](#) | [METHODOLOGY](#) | [TEAM](#) | [ADVERTISE WITH US](#) | [CONTACT US](#) | [SITEMAP](#) | [SUBSCRIBE](#)
| [NEWSLETTER](#)
[DIGITAL EDITION](#) | [AUTHORS](#) | [EXTERNAL CONTRIBUTORS](#) | [TOP LAWYERS](#) | [LEGAL FAQ](#) | [PREMIUM](#)



LEXPERT
BUSINESS OF LAW

