Privacy and Data Protection Laws in Canada and Canada's Anti-Spam Legislation

Doing Business in Canada

AIRD BERLIS

2025 EDITION

airdberlis.com

Canada has well-established federal and provincial privacy and data protection statutes, in both private and public sectors, as well as growing protection over privacy rights throughout the common law.

Data breaches in Canada are evolving as a significant area of law relating to prevention, response (governmental and public) and litigation. Class action lawsuits involving data breaches are a growing response to data breaches in Canada and the damages awards have increased the exposure of businesses in Canada accordingly.

Privacy laws across Canada, at both the federal and provincial levels, are undergoing significant changes. Recent amendments to Quebec's provincial legislation, now fully in force, provide individuals with significantly enhanced rights and impose increased obligations and risks to organizations. These changes largely take effect over three years, starting in September 2022. As of September 2022, the following provisions in Quebec's amended privacy laws took effect: *Designation of a person in charge of the protection of personal information for an organization, mandatory reporting of confidentiality incidents, provisions governing the communication of personal information in the context of a commercial transaction and communication of personal information for research purposes*.

As of September 2023, the majority of the proposed revisions took effect, including the following: *Requirements surrounding governance policies and practices, privacy impact assessments, transparency and privacy notices, restrictions around using identification, geolocation tracking and profiling technologies, new consent requirements, privacy by default design requirements, requirements surrounding automated decision-making, regulations surrounding transfers of personal information outside of Quebec, requirements surrounding retention and destruction of personal information, creation of the right to be forgotten as well as the notable enforcement mechanisms*.

As of September 2024, *obligations surrounding data portability took effect*.

The Canadian federal government previously introduced draft legislation, the *Digital Charter Implementation Act*, designed in part to replace the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"). The *Digital Charter Implementation Act* would implement three different pieces of legislation significantly impacting privacy rights: (i) the *Consumer Privacy Protection Act* ("**CPPA**"); (ii) the *Personal Information and Data Protection Tribunal Act* ("**PIDPTA**"); and (iii) the *Artificial Intelligence and Data Act* ("**AIDA**"). This draft legislation died on the order table during the last federal election. It's not clear whether the new government will re-table this or similar legislation; however, we expect legislation similar to those proposed under the CPPA. We also expect an effort to separate the proposed CPPA and PIDPTA from those under AIDA, as the AIDA provisions faced significant industry challenges in their earlier form.

In the draft form, the CPPA would take the place of Part 1 of PIPEDA and would include significant changes to permitted information handling practices, establish additional rights to individuals and increase the powers of the Office of the Privacy Commissioner of Canada. The PIDPTA, when in force and effect, would establish an administrative tribunal to hear appeals of certain decisions made by the privacy commissioner under the CPPA and impose penalties for the contravention of certain provisions of that Act. AIDA regulates international and interprovincial trade and commerce in artificial intelligence systems by requiring that certain persons adopt measures to mitigate risks of harm and biased output related to high-impact artificial intelligence systems.

AIDA would have mandated public reporting of AI systems and risks in certain instances and authorizes the Minister to order the production of records related to artificial intelligence systems. AIDA would have also established prohibitions related to the possession or use of illegally obtained personal information for the purpose of designing, developing, using or making available for use an artificial intelligence system, and to the making available for use of an artificial intelligence system if its use causes serious harm to individuals. There were significant challenges to the AIDA as drafted, due in part to the vagueness of its application.

In November 2023, the federal government proposed amendments to AIDA, which we believe will be captured in some manner under new AI legislation introduced by the current government. The proposed amendments include:

- a new definition of "artificial intelligence systems" that takes after the definition of the Organization of Economic Co-operation and Development, and a new definition of "machine learning model";
- an initial list of high-impact AI systems, such as content moderation and prioritization on communications platforms (e.g., social media and search engines), employment-related decisions, biometric information processing, healthcare and emergency services and law enforcement;

- new powers for the Artificial Intelligence and Data Commissioner, such as inspections, audits and compelling companies to produce assessments required under AIDA; and
- alignment of AIDA with the European Union's *Artificial Intelligence Act* ("**EU AI Act**").

The European Union Parliament voted in favour of the EU AI Act on March 13, 2024. The EU AI Act may potentially impact Canadian companies exporting AI-enhanced regulated products or systems used in high-risk areas within the European Union. These companies will be compelled to adhere to intricate new compliance regulations. Moreover, Canadian businesses providing online services with AI components accessible to EU consumers may also be affected.

Additionally, the Province of Ontario underwent a consultation process to determine whether it should introduce new privacy legislation which, if introduced, would significantly change the rights and obligations under privacy laws within the province. Additional provinces across Canada are also reviewing their privacy legislation (or lack thereof) with a view to co-ordinating with their provincial and federal counterparts. Please keep these processes in mind when reviewing the following summary of privacy laws.

Given requirements from the European Union and the Quebec legislation requiring substantially similar protections to personal information to permit data transfers, we expect the various pieces of legislation at the federal and provincial level to have many similarities.

Canadian businesses are often subject to multiple pieces of legislation at the federal and provincial levels that protect the privacy rights of individuals. For instance, PIPEDA regulates the collection, use and disclosure of personal information ("**Personal Information**") in the course of "commercial activities." Legislation substantially similar to PIPEDA exists in various provinces, including British Columbia's *Personal Information Protection Act*, S.B.C. 2003 c. 63, Alberta's *Personal Information Protection Act*, S.A. 2003, c. P-6.5, and Quebec's *Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1.

Various provinces have also enacted legislation which regulates the collection, use and disclosure of personal health information. Most notably, *Ontario's Personal Health Information Protection Act* ("**PHIPA**") regulates personal health information when collected, used or disclosed to health information custodians in the provision of providing health care.

Depending on the nature of an organization's activities and the use made of Personal Information, compliance involves complex processes such as privacy audits and data mapping, privacy impact assessments for new undertakings involving Personal Information, staff training, implementation of security systems, improvements to storage systems, development of privacy policies (internal and external) and the implementation of other protective measures, including ensuring contractual provisions exist with third parties who may have access to the Personal Information in the organization's possession or control.

Canadian privacy considerations affect an organization expanding into or operating in Canada in a few ways:

First, an organization itself will have to comply with PIPEDA and other privacy legislation with respect to Personal Information that it collects, uses, discloses, stores or otherwise processes on individuals who are not employees of the organization (unless the organization is federally regulated). Organizations will also have to also comply with privacy legislation in relation to its employee information for federally regulated organizations. To the extent a provincially regulated organization has employees located in the provinces of British Columbia, Alberta or Quebec, or otherwise has Personal Information on residents of those provinces, it will need to consider the impact of such provincial privacy laws on Personal Information.

Secondly, organizations will want to ensure that all third parties to whom they grant access to, or use of, the Personal Information have undertaken personal impact assessments to determine whether the privacy rights afforded in their jurisdiction will be upheld by the third parties who have access to otherwise process the Personal Information. The privacy impact assessment involves due diligence on the third party's practices, controls and safeguards, as well as an understanding of the laws that apply to the third party which may undermine the third party's ability to properly protect the Personal Information, contractual provisions in place regulating the third party's use, disclosure and security around the Personal Information, and certain audit rights to ensure such third party complies with its obligations. Thirdly, organizations will need to have plans in place to prevent data breaches, including technological measures and human resources training for employees, contractors and every third party who may have access to their systems. Finally, organizations will need to have a breach response plan in place for the inevitable data incursion and/or data breach. Such response

plans should include the appropriate members of the breach response team, including third parties to assist, such as IT forensic, insurance, and public response organizations.

Many privacy laws across Canada at the federal and provincial level impose mandatory breach notification requirements. For example, businesses subject to PIPEDA have an obligation to report a privacy breach to the Office of the Privacy Commissioner of Canada and the individuals whose information has been breached if there is a reasonable risk of significant harm resulting from the breach, as well as obligations in certain circumstances to report privacy breaches to third-party organizations. In addition, there are extensive record-keeping obligations pertaining to all privacy breaches, not just those that are reported, for organizations subject to PIPEDA.

Overview of PIPEDA

The purpose of PIPEDA, as with other privacy laws across Canada, is to balance the right of privacy of individuals with the need of businesses to use Personal Information for reasonable purposes in order to operate successfully. "Personal Information" is specifically defined as "information about an identifiable individual." It does not include certain business contact information. It includes such information as race, ethnic origin, colour, age, marital status, religion, education, medical, criminal, employment or financial history, address and telephone number, Social Insurance Number, fingerprints, blood type, tissue or biological sample and views or personal opinions that are linked to an individual. In a recent landmark decision, the Supreme Court of Canada ruled that internet protocol ("**IP**") addresses attract a reasonable expectation of privacy. This is because they can reveal deeply personal information about individuals, including their identity, as contained in or inferred from their internet activity, particularly when combined with other information or data sets.

PIPEDA applies to organizations in Canada that collect, use or disclose Personal Information in the course of all commercial activity. "Commercial activities" are defined to mean "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character."

While some people may believe that the legislation applies only to organizations with a business in Canada, the Federal Court of Canada has held that the federal privacy commissioner has a broad right to investigate organizations that collect, use or disclose personal information of Canadians.

What Does an Organization Need to Do?

PIPEDA outlines several key principles to protect Personal Information. It also requires that Personal Information be used or disclosed only for purposes for which it was collected. Once an organization collects Personal Information, it maintains ongoing obligations with respect to its use and safeguarding.

Obtain Informed and Meaningful Consent: The foundation of PIPEDA and all of Canada's privacy laws is to obtain informed, meaningful consent for the collection, use and disclosure of Personal Information. Historically, Canada has relied more heavily on implied consent to satisfy the consent requirements. However, privacy commissioners across Canada are moving toward requiring express consent (positive opt-in model) to establish informed and meaningful consent.

Be Accountable: An organization must be responsible for Personal Information under its control and shall designate an individual or individuals who is/are accountable for the organization's compliance with the following principles. The obligation to be accountable continues to apply even if the organization outsources certain functionalities to third parties and organizations must ensure that the third parties to whom Personal Information is disclosed or to whom access to Personal Information is given adhere to Canadian privacy laws.

Identify the Purpose: The purposes for which Personal Information is collected shall be identified by the organization at or before the time the information is collected. This is a broad obligation and, in addition to the more common purposes for which data is collected, organizations should also identify practices such as using artificial intelligence and/or predictive behaviour mechanisms, as well as rights to deidentify personal information and commercialize such data to third parties.

Be Accurate: Personal Information shall be accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Be Open: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of Personal Information.

Give Individuals Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her Personal Information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Secure Personal Information: Ensure appropriate security safeguards are in place to secure the Personal Information.

Notification of Breach: Where there is a breach of security safeguards, or a failure to implement appropriate security safeguards, the organization has an obligation to notify the Office of the Privacy Commissioner of Canada and the individuals whose information has been breached if there is a reasonable risk of significant harm resulting from the breach, as well as obligations in certain circumstances to report privacy breaches to third party organizations.

Record Keeping: There are extensive record keeping obligations pertaining to all privacy breaches, not just those that are reported, for organizations subject to PIPEDA.

Provide Recourse: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

What Are the Risks if an Organization Does Not Comply?

Breaches of privacy legislation can impose both statutory and common law liability. Penalties under the *Quebec Act* and proposed under the *Digital Charter Implementation Act* can result in fines and penalties of several millions of dollars.

Until a replacement for the *Digital Charter Implementation Act* is in force and effect, complaints by individuals under PIPEDA, the current regime, are heard by the federal privacy commissioner who has the authority to receive and investigate complaints and to try to resolve these disputes (similarly, complaints in the provinces are heard by the relevant provincial privacy commissioner). The privacy commissioner also has the right to make public any information relating to an organization's Personal Information management practices if it is in the public interest to do so. Public disclosure of the details of the complaint can be the most damaging to a business, and is a destructive consequence of misusing Personal Information. The individual making the complaint can also apply to court for damages.

PIPEDA creates offences for obstructing an investigation or audit; destroying Personal Information that is the subject of an access request; or disciplining a whistleblower.

An organization that engages in these activities can be fined up to $10,000 for a summary conviction or $100,000 for an indictable offence.

Persons can also seek remedies from court for breaching PIPEDA, other privacy statutes and common law obligations. While individual damage awards have been somewhat limited to date for breaching privacy rights, the courts are expanding these damage awards and are more accepting to certifying class action lawsuits relating to breaches of individuals' privacy rights.

Processing of Personal Information in the United States

As indicated above, an organization has an obligation to safeguard the Personal Information processes and not to disclose it to third parties without consent.

There is a sensitivity in Canada regarding the outsourcing of any data management services outside the country. Many concerns can be dealt with by undertaking personal impact assessments to understand the risk involved in outsourcing to the third party, selecting third parties with appropriate safeguards to address safeguarding obligations, ensuring adequate data protection agreements are in place with the third parties, and ensuring appropriate notice requirements with individuals are satisfied. However, legislation exists in certain provinces which applies to the public sector and prohibits the disclosure of storage or access to Personal Information outside of Canada.

Data Breach Notification in Canada

Arguably, Canada has had breach notification obligations for as long as privacy laws existed. An organization is not able to use or disclose Personal Information for purposes that had not previously been consented to by the individual without such individual's notice and consent. However, to clarify and to formalize this, PIPEDA and *Alberta's Personal Information Protection Act* ("**PIPA**") have mandatory breach notification obligations, as does PHIPA. Quebec also has breach notification obligations. Businesses subject to PIPEDA, PIPA, PHIPA and Quebec's Act respecting the protection of personal information in the private sector (enforced by the Commission d'accès à l'information, or **CAI**) have an obligation to report a privacy breach to the regulator in their respective jurisdictions in certain circumstances. For example, organizations subject to PIPEDA and PIPA need to notify regulators and the individuals whose information has been breached if there is a reasonable risk of significant harm resulting from the breach, as well as obligations in certain circumstances to report privacy breaches to third-party organizations. In addition, there are extensive record-keeping obligations pertaining to

all privacy breaches, not just those that are reported, for organizations subject to PIPEDA.

Common Law Right to Privacy

The common law tort of invasion of privacy continues to develop throughout Canada and the provinces in various ways. For example, in the last few years, Ontario has recognized the common law torts referred to as Intrusion on Seclusion, Public Disclosure of Private Facts and Publicity Placing a Person In False Light. While the courts initially limited the damages to approximately $20,000 for a breach, except in extraordinary circumstances, in recent months the courts appear more willing to increase the damage awards for an individual breach to more substantive dollar values.

Canada's Anti-Spam Legislation

Anti-spam legislation in Canada has been in force since 2014 (*An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*) ("**CASL**"). CASL is arguably one of the strictest regimes in the world regulating the communication of commercial electronic messages in terms of the scope of application, requirements and the penalties imposed upon failure to comply. The legislation requires businesses to comply with its requirements surrounding the sending and disseminating of commercial electronic messages ("**CEMs**"), including its strict consent and detailed content obligations. This legislation has extremely broad application and includes CEMs sent via email, text, SMS, BBM and direct social media communications. CEMs are considered to be messages that encourage participation in a commercial activity and include offering, advertising or promoting a product or service.

In 2015, further provisions concerning the unsolicited installation of computer programs and software came into force. These provisions prohibit the installation of a computer program to another person's computing device (such as a smartphone, laptop or other connected device) in the course of commercial activity without the express consent of the device owner or an authorized user.

The Competition Bureau and the Office of the Privacy Commissioner of Canada jointly enforce Canada's anti-spam legislation. The legislation is enforced through regulatory measures, including significant administrative monetary penalties. Businesses and individuals who are subject to the legislation, including directors, officers and agents, that do not comply risk significant financial penalties that can range up to $1 million per violation for individuals and $10 million for businesses. CASL was supposed to statutorily permit a private right of action for breaching its terms as of July 1, 2017, which would have created further financial repercussions for violations of the legislation. However, the effective date for the statutory private right of action has been postponed indefinitely.

June 2025

AIRD BERLIS

We are committed to being the Canadian gateway for our clients.

Brookfield Place, 181 Bay Street, Suite 1800, Toronto, ON M5J 2T9
T 1.416.863.1500 F 1.416.863.1515

701 West Georgia Street, Suite 1420, Vancouver, BC V7Y 1E4
T 778.371.2241 F 778.371.2270

Other articles and papers written by our professionals can be viewed at:

airdberlis.com

Doing Business in Canada offers general comments on legal developments of concern to businesses, organizations and individuals, and is not intended to provide legal opinions. Readers should seek professional legal advice on the particular issues that concern them.