PRIVACY LAWS

By Eugen Miscoi, Jon Adessky and Pierre Dushime

PRIVACY LAWS

Summary

All businesses in Canada are subject to legislation that regulates the collection, use and disclosure of personal information in the course of commercial activity and in some jurisdictions, in the management of employees. "Personal information" generally means information about an identifiable individual. The collection, use and disclosure of personal information by private sector organizations within the provinces of British Columbia, Alberta and Québec are regulated by legislation enacted by each of those provinces, while a federal private sector privacy law governs the collection and processing of personal information in the rest of Canada.

ALL BUSINESSES IN CANADA ARE SUBJECT TO LEGISLATION THAT REGULATES THE COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION IN THE COURSE OF COMMERCIAL ACTIVITY.

These statutory regimes are all generally built upon the following 10 principles that govern the collection, use and disclosure of personal information:

— accountability;

— identifying purposes;

— consent;

— limiting collection;

— limiting use, disclosure and retention;

— accuracy;

— security safeguards;

— openness;

— individual access; and

— challenging compliance.

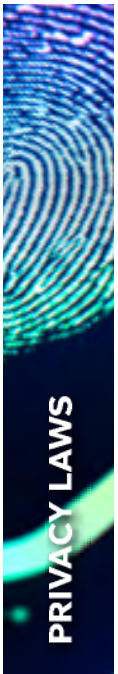
In addition to general private sector privacy laws, Alberta, Manitoba, Nova Scotia, New Brunswick, Newfoundland and Labrador, Ontario, Québec and Saskatchewan also have specific health privacy legislation to protect personal health information. For example, Ontario's *Personal*

Health Information Protection Act, 2004 establishes rules for the collection, use and disclosure of personal health information by health information custodians in Ontario.

Federal Private Sector Privacy Law — PIPEDA

At the federal level, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs the collection, use and disclosure of personal information in provinces and in the territories that have not adopted substantially similar privacy legislation, as well as in the course of interprovincial and international commercial activities. PIPEDA applies to all federally regulated works, undertakings or businesses, regardless of the province in which they operate. This includes entities such as banks, airlines, telecommunications service providers and other organizations operating under federal jurisdiction. As outlined in greater detail below, if and when the *Consumer Privacy Protection Act* (CPPA) — introduced by *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* (Bill C-27) is adopted, the regime for the protection of personal information set out in PIPEDA will be modernized to bring it in close alignment with Québec's Act to *modernize legislative provisions respecting the protection of personal* information (Law 25 and formerly known as Bill 64).

Unless certain exceptions apply, an individual's knowledge and consent are required to collect, use or disclose their personal information. Explicit consent may be required for more sensitive personal information (e.g., medical or financial information), while implicit consent may be sufficient for non-sensitive personal information (e.g., mailing address). Pursuant to amendments to PIPEDA adopted in 2015, the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. Exceptions to the "consent" requirement include disclosures of personal information in the context of certain business transactions, as defined in the law.



The Office of the Privacy Commissioner's (OPC) *Guidelines for Obtaining Meaningful Consent* (Guidelines) clarify that failure to obtain meaningful consent may lead a business to lose its ability to handle personal information needed to operate the business. In order to obtain meaningful consent, businesses are encouraged to: (i) ensure that their privacy policy is written in plain language; (ii) use just-in-time privacy notices on their website as a supplement to the longer form privacy policy; (iii) prepare an executive summary of their privacy policy's key highlights to place at the top of the privacy policy; and (iv) use interactive tools in the presentation of their privacy information.

Provincial Privacy Laws

Alberta, British Columbia and Québec have adopted their own private sector privacy laws that may apply instead of PIPEDA for both consumer and employee personal information practices of organizations within these provinces. These laws have been deemed substantially similar to PIPEDA. As such, the following section offers a comprehensive overview of Québec's privacy regime, focusing solely on this province due to the fact that it establishes some of the most stringent requirements applicable in Canada. In other words, complying with Québec's privacy regime ensures material compliance with other privacy regimes across the country.

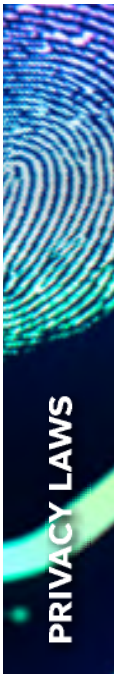
Québec

The *Act respecting the protection of personal information in the private sector* (Québec Act) applies to the collection, use or disclosure (referred to as 'communication') of personal information within the province by 'any person carrying on an enterprise'. This privacy regime has gone — and continues to go through — amendments introduced by Law 25. Table 1 below summarizes key new obligations brought forth by Law 25, organized by their entry into force date.

Table 1: Summary of Amendments and Timeline of Entry Into Force Dates

SEPTEMBER 22, 2022:	SEPTEMBER 22, 2023:	SEPTEMBER 22, 2024:

New Obligations
— Appointment of a Privacy Officer
— Mandatory Breach Reporting
— Consent exceptions for:
  — Commercial Transactions; and
  — Study, Research, or Statistics
— Disclosure of biometric databases for authentication to Québec's Commission d'accès à l'information (CAI)
	New Obligations
	— Privacy Framework
	— Additional transparency requirements
	— Privacy Impact Assessments
	— Privacy by default and by design
	— De-indexation rights
	— Additional consent requirements
	— Cross-border transfers of personal information
	— New regime for the secondary use of personal information
	— Strict retention and destruction obligations
	— New obligation when an automated decision is made using an individual's personal information
	— New regime for business contact information
	— New sanctions for non-compliance
		New Obligations
		— Right to Data Portability



A significant development brought forth by Law 25 are the monetary fines that could result from non-compliance with the Québec Act. Effective September 22, 2023, the CAI may impose an administrative monetary fine for non-compliance of up to C$10 million or 2% of worldwide turnover for the preceding fiscal year, whichever is greater. Alternatively, the CAI can institute court proceedings with potential maximum penal fines of up to C$25 million or 4% of worldwide turnover the preceding fiscal year, whichever is greater. In the case of subsequent non-compliance, fines may be doubled. The CAI's **General Framework for Application of MAPs** determines initial fines for various levels of non-compliance, which is used to classify the severity of non-compliance into four categories: minor, moderate, serious, and very serious.

This categorization determines the base penalty. Subsequently, the CAI adjusts the base amount based on factors like the non-compliance's nature, potential harm, and data sensitivity. Thus, the base amounts are not minimum and may be lower if mitigating factors exist. However, fines can substantially increase with aggravating factors, up to C$10 million or 2% of an organization's prior-year global turnover, whichever is larger.

Key Trends in Canadian Privacy Laws

Privacy breach notifications and record keeping

For many years, *Alberta's Personal Information Protection Act* (Alberta PIPA) was the only general private sector privacy law in Canada that imposed a statutory obligation on private sector organizations to report privacy breaches. Under Alberta PIPA, organizations must only report (to the Information and Privacy Commissioner of Alberta) privacy breaches that could pose a "real risk of significant harm to an individual." The Information and Privacy Commissioner of Alberta in turn determines whether an organization needs to notify the individuals affected.

As of November 1, 2018, due to amendments made to PIPEDA by virtue of the *Digital Privacy Act*, organizations across Canada must comply with new mandatory breach notification rules. Organizations subject to PIPEDA have reporting, notice and record retention obligations for any breach of security safeguards. A breach of security safeguards is broadly defined as: "the loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards." Reporting and notification obligations are triggered when there is a real risk of significant harm to an individual (RROSH). RROSH is also broadly defined and includes "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property." The factors that are relevant to determine whether a breach creates a RROSH include the sensitivity of the personal information involved in the breach of security safeguards, as well as the probability that the personal information has been, is, and/or will be misused.

The report of the breach to the OPC must be made "as soon as feasible after the organization determines that the breach has occurred." The same criteria apply for notifying individuals of breaches involving their personal information unless the law provides otherwise.

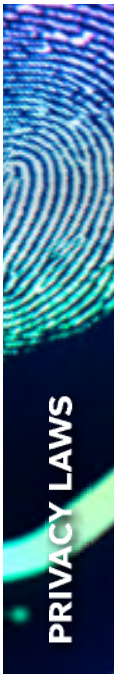
The notification needs to be conspicuous and contain sufficient information to help affected individuals mitigate the risk of harm. Information as to what information should be included in written reports to the OPC and individual notifications can be found in the *Breach of Security Safeguards Regulations*. Furthermore, whether or not there is a RROSH, an organization must keep a security-breach log for 24 months following a breach of security safeguards. During this period, organizations must comply with requests from the OPC to have access to the record at any time. Further, an organization encountering a breach will have additional reporting obligations to other organizations and government institutions if the breached organization believes the other organizations may be able to reduce their risk of harm as a result.

Organizations subject to PIPEDA face liability for knowingly violating the notification requirements. An organization may be liable for fines up to C$100,000 per violation. In addition, PIPEDA provides the federal privacy commissioner with the right to make public any information that comes to his or her attention in the performance or exercise of any of his or her duties, as well as make public any information in security-breach notification reports to the OPC, if he or she judges there is a public interest for doing so. Overall, these provisions introduce more stringent privacy, consent and breach notification obligations.

In Québec, Law 25 has introduced new notification requirements for private sector companies who are the target of a privacy breach, or as referred to in Law 25 as a "confidentiality incident." A confidentiality Incident is defined as an unauthorized access, use, or communication of personal Information, loss of personal information, or any breach in the protection of such information. In the event of a confidentiality incident that poses a "risk of serious injury," companies are obligated to take reasonable measures to mitigate the risk and prevent similar incidents. Determining whether a specific incident poses a "risk of serious injury" depends on several factors, including the sensitivity of the information involved, the potential consequences that may arise from its use and the likelihood that the information will be utilized for harmful purposes. In the occurrence of a "risk of serious injury," organizations are obligated to promptly notify both the CAI and the individuals who are affected.

Cross-Border Data Transfer

With respect to transfers of personal information to service providers located outside Canada, the "openness" principle under PIPEDA has



been held by federal privacy regulators to require that notice of such transfers should be provided to affected individuals. Alberta PIPA requires that organizations notify individuals if they transfer personal information to a service provider located outside Canada. In Québec, effective from September 22, 2023, Law 25 brings forth new obligations for businesses involved in cross-border transfers of personal information. At the time the information is collected and on request, businesses must inform individuals of the possibility that the information collected may be communicated outside Québec. Before communicating personal information outside of Québec, a cross-border privacy impact assessment must be conducted to establish that the information transferred will receive adequate protection in the target transfer jurisdiction. The assessment considers factors such as the sensitivity of the information, intended purposes, protection measures, and the legal framework of the receiving jurisdiction. Cross-border transfers must also be the subject of a written agreement that takes into account the results of the assessment, and terms agreed upon that mitigate risks. It is worth noting that these requirements apply equally between interprovincial and international transfers of personal information.

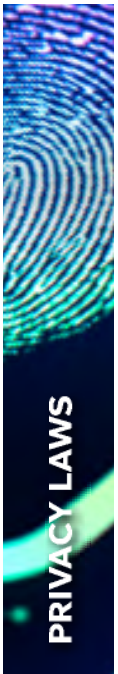
Guidelines for Businesses

Whether PIPEDA or similar provincial legislation is the applicable privacy regime, immediate priorities for most organizations that establish a business in Canada should be:

- the adoption of a documented privacy compliance strategy that identifies the organization's compliance with the applicable regulatory regimes;
- the adoption of an external and internal privacy policy, and personal information management practices to ensure compliance with applicable privacy laws;
- the appointment of an individual who will be responsible for the administration and oversight of the organization's personal information management practices and who will be prepared to implement any changes required by applicable legislation;

IMMEDIATE PRIORITIES FOR MOST ORGANIZATIONS THAT ESTABLISH A BUSINESS IN CANADA SHOULD INCLUDE THE APPOINTMENT OF AN INDIVIDUAL WHO WILL BE RESPONSIBLE FOR THE ADMINISTRATION AND OVERSIGHT OF THE ORGANIZATION'S PERSONAL INFORMATION MANAGEMENT PRACTICES.

- a review of the current personal information practices of the organization outside Canada and proposed information practices within Canada, including determining what personal information is collected, and from where; what consents are obtained and what purposes are identified when collecting personal information; where personal information is stored; how personal information is used; when and to whom personal information is disclosed; and how current personal information practices of the organization may need to be changed for the collection, use and disclosure of personal information in Canada;
- a review of the organization's data management infrastructure to ensure that the infrastructure is adequately flexible and robust to facilitate the implementation of the organization's privacy policies and data management practices;
- the implementation of consent language in contracts, forms (including Web forms) and other documents utilized when collecting personal information from individuals (including customers and employees);
- a review of agreements to ensure that where there are contracts with third parties to whom personal information will be disclosed (or where the third party is granted access to the personal information), that the third party agrees to appropriate contractual terms, such as: specifying the ownership of the data and ensuring that the third party will provide adequate security safeguards for the information; ensuring that the personal information will be used only for the purposes for which it was disclosed to the third party; ensuring that the third party will cease using (and return or destroy) the personal information if requested; and providing for indemnification by the third party for any breach of such terms;
- the preparation of privacy impact assessments to adequately assess risks to personal information for new projects and cross-border data transfers; and
- the adoption of a privacy breach response plan that clearly specifies internal contacts and external advisors so that there is no mistake about who is to be contacted for immediate support in the case of an incident. An organization must be able to quickly identify a privacy breach, immediately carry out its plan of action, isolate the affected systems, determine the damage and remediate.



Implementation of such initial steps may require several months, depending on the size and maturity of the organization.

Non-compliance

Compliance with privacy laws needs to be considered in any business transaction involving the disclosure or transfer of personal information, such as purchases or sales of businesses, outsourcing transactions and securitization transactions. For example, when considering the acquisition of a business in Canada, it is crucial that a review of the target company's privacy policies and practices be included as part of the due diligence process. If personal information of employees or customers has to be disclosed to the purchaser during the due diligence process, it is also essential that an appropriate confidentiality regime be established for the process. It is recommended that only personal information that is necessary or likely to affect the decision to proceed with a transaction or its terms (including price) be disclosed.

Failure to comply with privacy laws can result in complaints to the relevant privacy commissioner, orders and fines. An organization with deficient privacy practices may risk adverse publicity for failure to comply with privacy laws.

Law 25 introduces new consequences for non-compliance for businesses with operations in Québec. See **Québec**.

In light of the complexity of privacy laws and the differences between the various laws that may apply to an organization or to a particular business unit, ensuring privacy compliance across an organization's departments may be challenging, particularly for organizations that operate globally.

It is important to note that these exceptions to consent in case of emergency situations can vary across Canadian privacy statues and may contain certain conditions. Generally, a notice of disclosure should be given to the individual before or without delay after the fact, if possible. In addition, these legislative authorizations do not always apply to "regular" business operations. Organizations are therefore encouraged to take into account applicable laws, before applying legislative authorizations that provide exemptions to the requirement to obtain consent for the collection, use and disclosure of personal information. Finally, the COVID-19 pandemic also raised concerns regarding information security aimed particularly at remote working arrangements. In order to meet

their privacy obligations, organizations must take all the reasonable steps to ensure that the data is protected appropriately from theft, loss, unauthorized disclosure and other compromise.

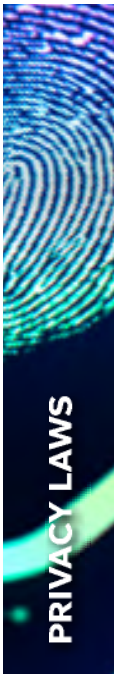
Upcoming and Ongoing Changes to the Canadian Privacy Regime

Canadian federal and provincial governments have been advancing bills and passing legislation to modernize the privacy landscape under their respective jurisdictions.

— Federally, Bill C-27 seeks to modernize the federal privacy regime. As such, Bill C-27 creates three new acts: (i) the CPPA, which replaces the privacy sections of the current federal private sector privacy law, PIPEDA; (ii) the *Personal Information and Data Protection Tribunal Act* (PIDPTA), which would create an appeals tribunal for privacy decisions under the CPPA; and (iii) the *Artificial Intelligence and Data Act* (AIDA), which would be Canada's first law that directly regulates artificial intelligence. Bill C-27 is making its way through the federal legislative process and is likely to evolve before its three new acts become law (if and when they do).

— Provincially, the Québec Act has been overhauled by Law 25. Law 25 received royal assent on September 22, 2021, and significantly changes Québec's privacy regime via a three-phased entry into force of its European-style framework on September 22 of 2022, 2023 and 2024.

These modernization efforts are unfolding in the context of a broader global movement toward ever-increasing privacy obligations for organizations that collect and process personal information in the context of their operations. Please contact our multidisciplinary Cyber/Data Group for practical advice on how to efficiently stay on top of all applicable requirements in Canada.



FOR MORE INFORMATION, PLEASE CONTACT:

Charles S. Morgan
cmorgan@mccarthy.ca
514-397-4230

Dan Glover
dglover@mccarthy.ca
416-601-8069