

DATA PROTECTION LAWS OF THE WORLD

Canada



Downloaded: 25 April 2024

CANADA



Last modified 26 January 2023

LAW

In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, criminal code provisions etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

The summary below focuses on Canada's private sector privacy statutes:

- Personal Information Protection and Electronic Documents Act ('PIPEDA')
- Personal Information Protection Act (Alberta) ('PIPA Alberta')
- Personal Information Protection Act (British Columbia) ('PIPA BC')
- Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Private Sector Act'), (collectively, 'Canadian Privacy Statutes')

On June 16, 2022, the federal Government introduced Bill C-27, a wide-reaching piece of legislation that is intended to modernize and strengthen privacy protection for Canadian consumers and provide clear rules for private-sector organizations. It is the second attempt to modernize federal private-sector privacy legislation, after a previous proposal died on the order paper in 2021. If adopted, Bill C-27 will replace PIPEDA with legislation specific to consumer privacy rights (the *Consumer Privacy Protection Act*) and electronic documents (the *Electronic Documents Act*). Bill C-27 will also introduce the *Artificial Intelligence and Data Act*, which aims to create rules around the deployment of AI technologies.

Key elements of Bill C-27 include:

- Clarified consent requirements for the collection, use and disclosure of personal information
- Expanded enforcement powers for the Office of the Privacy Commissioner of Canada, including stiff penalties for serious offenses of up to 5% of annual gross global revenue or CA\$25 million
- New rules governing de-identified information
- The creation of a specialized Personal Information and Data Protection Tribunal

C-27 is currently at the committee stage of the legislative process. There has been considerable debate over the Bill, in particular over the proposed *Artificial Intelligence and Data Act*. The final form of the language remains subject to material change.

PIPEDA applies to all of the following:

- Consumer and employee personal information practices of organizations that are deemed to be a federal work, undertaking or business; (eg, banks, telecommunications companies, airlines, railways, and other interprovincial undertakings)
- Organizations who collect, use and disclose personal information in the course of a commercial activity which takes place

within a province, unless the province has enacted substantially similar legislation (PIPA BC, PIPA Alberta and the Quebec Private Sector Act have been deemed substantially similar;)

- Inter provincial and international collection, use and disclosure of personal information in connection with commercial activity

PIPA BC, PIPA Alberta and the Quebec Private Sector Act apply to both consumer and employee personal information practices of organizations within BC, Alberta and Quebec, respectively, that are not otherwise governed by PIPEDA.

Quebec recently enacted a major reform of its privacy legislation with the adoption of Bill 64. Bill 64 received Royal Assent on September 22, 2021. A first set of amendments came into force on September 22, 2022, with additional modifications set to come into force on September 22, 2022, while the majority of substantial changes came into force on September 22, 2023. A third, more limited set of amendments will come into force on September 22, 2024. With Bill 64's changes, Quebec now has in place a sophisticated legal framework for privacy and data protection that resembles the European GDPR in several key areas.

DEFINITIONS

Definition of personal data

Personal information includes any information about an identifiable individual (business contact information is expressly carved out of the definition of personal information in some Canadian privacy statutes).

The Quebec Private Sector Act, as modified by Bill 64, has broadened the definition of personal information to include any information that allows an individual to be identified indirectly as well as directly. In Quebec, business contact information is included in the definition of personal information, however it is considered a less sensitive form of data to which many of the requirements of the Quebec Private Sector Act do not apply.

Definition of sensitive personal data

Not specifically defined in Canadian Privacy Statutes, except for the Quebec Private Sector Act.

The Quebec Private Sector Act, as modified by Bill 64, defines sensitive personal information as any information that, by virtue of its nature (e.g. biometric or medical), or because of the context in which it is used or communicated, warrants a high expectation of privacy. The Quebec Privacy Act has stricter consent requirements in certain situations for the use and communication of personal information qualified as sensitive.

Definition of anonymized information

The Quebec Private Sector Act, as modified by Bill 64, defines anonymized information as information concerning an individual which irreversibly no longer allows such individual to be identified, whether directly or indirectly. Quebec recently adopted a regulation which prescribes certain criteria and procedures which must be followed when anonymizing data.

Definition of de-identified information

The Quebec Private Sector Act, as modified by Bill 64, defines de-identified information as any information which no longer allows the concerned individual to be identified directly. De-identified information is still considered to be a form of personal information, to which most of the protections set out in the Quebec Private Sector Act continue to apply.

Definition of biometric information

The Quebec privacy regulator, the *Commission d'accès à l'information* (CAI), defines biometric information as information measured from a person's unique physical, behavioural or biological characteristics. Biometric information is, by definition, sensitive information.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Privacy Commissioner of Canada ('PIPEDA');

Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta');

Office of the Information and Privacy Commissioner for British Columbia ('PIPA BC'), and

Commission d'accès à l'information du Québec (the 'CAI') ('Quebec Private Sector Act');

REGISTRATION

There is no general registration requirement under Canadian Privacy Statutes.

Some registration requirements exist under Quebec privacy laws:

- Personal information agents, defined as any person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports; must be registered with the CAI
- The use of certain biometric systems and the creation of databases of biometric information must be disclosed to and registered with the CAI

DATA PROTECTION OFFICERS

PIPEDA, PIPA Alberta, and PIPA BC expressly require organizations to appoint an individual responsible for compliance with the obligations under the respective statutes.

The Quebec Private Sector Act, as modified by Bill 64, requires organizations to appoint a person responsible for the protection of personal information, who is in charge of ensuring compliance with privacy laws within the organization. By default, the person with the highest authority within the organization will be the person responsible for the protection of personal information, however this function can be delegated to any person, including a person outside of the organization.

This person's responsibilities are broadly defined in the law and include:

- Approval of the organization's privacy policy and practices
- Mandatory privacy impact assessments
- Responding to and reporting security breaches, and
- Responding to and enacting access and rectification rights

The contact information of the person responsible for the protection of personal information must be published online on the website of the organization.

COLLECTION & PROCESSING

Canadian Privacy Statutes set out the overriding obligation that organizations only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances;

Subject to certain limited exceptions prescribed in the Acts, consent is required for the collection, use and disclosure of personal information. Depending on the sensitivity of the personal information, consent may need to be presented as opt-in or opt-out. Under the Quebec Private Sector Act, consent must be clear, free and informed and be given for specific purposes; this is generally interpreted as requiring opt-in consent in most situations, however depending on the context and sensitivity of the information, opt-out or implicit consent may, in certain specific situations, be considered valid.

Organizations must limit the collection of personal information to that which is necessary to fulfil the identified purposes and only retain such personal information for as long as necessary to fulfil the purposes for which it was collected.

Each of the Canadian Privacy Statutes have both notice and openness/transparency requirements. With respect to notice, organizations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected. With respect to openness/transparency, generally Canadian Privacy Statutes require organizations make information about their personal information practices readily available.

All Canadian Privacy Statutes contain obligations on organizations to ensure personal information in their records is accurate and complete, particularly where the information is used to make a decision about the individual to whom the information relates or if the information is likely to be disclosed to another organization.

Each of the Canadian Privacy Statutes also provides individuals with the following:

- A right of access to personal information held by an organization, subject to limited exceptions;
- A right to correct inaccuracies in/update their personal information records; and
- A right to withdraw consent to the use or communication of personal information.

In addition to these rights, the Quebec Private Sector Act, as modified by Bill 64, gives individuals the right to have their personal information deindexed. A right to data portability will be coming into force on September 22, 2024.

Finally, organizations must have policies and practices in place that give effect to the requirements of the legislation and organizations must ensure that their employees are made aware of and trained with respect to such policies.

TRANSFER

When an organization transfers personal information to a third-party service provider (ie, who acts on behalf of the transferring organization -- although Canadian legislation does not use these terms, the transferring organization would be the controller; in GDPR parlance, and the service provider would be a processor;), the transferring organization remains accountable for the protection of that personal information and ensuring compliance with the applicable legislation, using contractual or other means. In particular, the transferring organization is responsible for ensuring (again, using contractual or other means) that the third party service provider appropriately safeguards the data, and would also be required under the notice and openness/transparency provisions to reference the use of third-party service providers in and outside of Canada in their privacy policies and procedures.

These concepts apply whether the party receiving the personal information is inside or outside Canada. Transferring personal information outside of Canada for storage or processing is generally permitted so long as the requirements discussed above are addressed, and the transferring party notifies individuals that their information may be transferred outside of Canada and may be subject to access by foreign governments, courts, law enforcement or regulatory agencies. This notice is typically provided through the transferring party's privacy policies.

With respect to the use of foreign service providers, PIPA Alberta specifically requires a transferring organization to include the following information in its privacy policies and procedures:

- The countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and
- The purposes for which the third party service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization

Under PIPA Alberta, specific notice must also be provided at the time of collection or transfer of the personal information and must specify:

- The way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and
- The name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service

providers outside Canada for or on behalf of the organization;

The Quebec Private Sector Act, as modified by Bill 64, requires all organizations to inform persons that their personal information may be transferred outside of Quebec: this is typically done at the time the information is collected. Additionally, before transferring personal information outside of the province of Quebec, organizations conduct data privacy assessments and enact appropriate contractual safeguards to ensure that the information will benefit from adequate protection in the jurisdiction of transfer. These assessments must take into account the sensitivity of the information, the purposes, the level of protection (contractual or otherwise) and the applicable privacy regime of the jurisdiction of transfer. Cross-border transfers may only occur if the organization is satisfied that the information would receive an adequate level of protection. Quebec has decided not to implement a system of adequacy decisions, and therefore assessments are required prior to any cross-jurisdiction transfer.

SECURITY

Each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organizations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. These laws do not generally mandate specific technical requirements for the safeguarding of personal information.

BREACH NOTIFICATION

Currently, PIPEDA, PIPA Alberta, and the Quebec Private Sector Act are the only Canadian Privacy Statutes with breach notification requirements;

In Alberta, an organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result.

Notification to the Commissioner must be in writing and include:

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date or time period during which the loss or unauthorized access or disclosure occurred
- A description of the personal information involved in the loss or unauthorized access or disclosure
- An assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure
- An estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm to individuals
- A description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure, and
- The name and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss of unauthorized access or disclosure

Where an organization suffers a loss of or unauthorized access to or disclosure of personal information as to which the organization is required to provide notice to the Commissioner, the Commissioner may require the organization to notify the individuals to whom there is a real risk of significant harm. This notification must be given directly to the individual (unless specified otherwise by the Commissioner) and include:

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date on which or time period during which the loss or unauthorized access or disclosure occurred
- A description of the personal information involved in the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm, and
- Contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure

The breach notification provisions under PIPEDA are very similar to the breach notification provisions under PIPA Alberta. The main difference is that PIPEDA requires organizations to notify both the affected individuals and the federal regulator if the breach creates a real risk of significant harm to the individuals (whereas PIPA Alberta requires the initial notice only to the regulator, and then to the individuals if the regulator requires it. In practice, many organizations notify affected Albertans regardless of whether the Alberta Commissioner requires (and the Commissioner typically does require it for most reported breaches in any event). Further, under PIPEDA, organizations must also keep a record of ALL information security breaches, even those which do not meet the risk threshold of a real risk of significant harm.

The Quebec Private Sector Act, as modified by Bill 64, introduced a number of new obligations in connection with confidentiality incidents, which are defined as unauthorized access, use, or communication of personal information, or the loss of such information, which were previously absent in Quebec privacy law. These include:

- A general obligation to prevent, mitigate and remedy security incidents
- The obligation to notify the CAI and the person affected whenever the incident presents a risk of serious injury. Factors to consider when evaluating the risk of serious injury include the sensitivity of the information concerned, the anticipated consequences of the use of the information and the likelihood that the information will be used for harmful purposes. Although the Quebec Private Sector Act requires organizations to act promptly and with diligence in response to confidentiality breaches, it does not provide specific timeframes within which such notifications must be made, and
- The obligation on to keep a register of confidentiality incidents, with the CAI having extensive audit rights

Quebec recently adopted regulations further detailing the reporting, notification, and record-keeping obligations of organizations in connection with confidentiality incidents.

ENFORCEMENT

Canadian privacy regulatory authorities have an obligation to investigate complaints, as well as the authority to initiate complaints.

Under PIPEDA, a complaint must be investigated by the Commissioner and a report will be prepared that includes the Commissioner's findings and recommendations. A complainant (but not the organization subject to the complaint) may apply to the Federal Court for a review of the findings and the court has authority to, among other things, order an organization to correct its practices and award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner resulting in an order. Organizations are required to comply with the order within a prescribed time period, or apply for judicial review. In both BC and Alberta, once an order is final, an affected individual has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the breach.

In Alberta and BC, a person that commits an offence may be subject to a fine of not more than CA\$100,000. Offences include, among other things, collecting, using and disclosing personal information in contravention of the Act (in Alberta only), disposing of personal information to evade an access request, obstructing the commissioner, and failing to comply with an order.

Similarly, under the Quebec Private Sector Act, an order from the CAI must be complied with within a prescribed time period. An individual may appeal to the judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.

The Quebec Private Sector Act, as modified by Bill 64, introduced a regime of steep fines and administrative penalties in case of non-compliance. The maximum penalties range between CA\$5,000 and CA\$100,000 in the case of individuals, and up to between CA\$15,000 and CA\$25 million or 4% of worldwide turnover for the preceding fiscal year for organizations. This new penalty regime represents a significant change with the previous Quebec regime, under which the maximum penalties were limited to CA\$20,000.

There are also statutory privacy torts in various provinces under separate legislation, and Ontario courts have recognized a

common-law cause of action for certain privacy torts. In Quebec, a general right to privacy also exists under the *Civil Code of Quebec* and the *Charter of Human Rights and Freedoms*. Organizations may face litigation (including class action litigation) under these statutory and common-law torts, as well as under the general regime of civil liability in Quebec, in addition to any enforcement or claims under Canadian Privacy Statutes.

ELECTRONIC MARKETING

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed above), as well as Canada's Anti-Spam Legislation (CASL);

CASL is a federal statute which prohibits sending, or causing or permitting to be sent, a commercial electronic message (defined broadly to include text, sound, voice, or image messages aimed at encouraging participation in a commercial activity) unless the recipient has provided express or implied consent and the message complies with the prescribed content and unsubscribe requirements (subject to limited exceptions).

What constitutes both permissible express and implied consent is defined in CASL and its regulations. For example, an organization may be able to rely on implied consent when there is an existing business relationship with the recipient of the message, based on:

- A purchase by the recipient within the past two years, or
- A contract between the organization and the recipient currently in existence or which expired within the past two years

CASL also prohibits the installation of a computer program on any other person's computer system, or having installed such a computer program to cause any electronic messages to be sent from that computer system, without express consent, if the relevant system or sender is located in Canada. In addition, the Act contains anti-phishing provisions that prohibit (without express consent) the alteration of transmission data in an electronic message such that the message is delivered to a destination other than (or in addition to) that specified by the sender;

CASL also introduced amendments to PIPEDA that restrict 'address harvesting', or the unauthorized collection of email addresses through automated means (i.e., using a computer program designed to generate or search for, and collect, email addresses) without consent. The use of an individual's email address collected through address harvesting also is restricted;

The 'Competition Act' was also amended to make it an offence to provide false or misleading representations in the sender information, subject matter information, or content of an electronic message;

CASL contains potentially stiff penalties, including administrative penalties of up to CA\$1 million per violation for individuals and CA\$10 million for corporations (subject to a due diligence defense). CASL also sets forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL (CA\$200 for each contravention up to a maximum of CA\$1 million each day for a violation of the provisions addressing unsolicited electronic messages). However, the private right of action is not yet in force, and there is currently little expectation that it will ever come into force;

ONLINE PRIVACY

Online privacy is governed by Canadian Privacy Statutes (discussed above). In general, Canadian privacy regulatory authorities have been active in addressing online privacy concerns;

For example, in the context of social media, the OPC has released numerous Reports of Findings addressing issues including:

- Default privacy settings
- Social plug-ins
- Identity authentication practices, including data scraping and voiceprint

- The collection, use and disclosure of personal information on social networking sites, including for marketing purposes;
- The OPC has also released decisions and guidance on privacy in the context of Mobile Apps

In addition, the OPC has released findings and guidelines related to the use of cookies and online behavioral advertising, including findings indicating that information stored by temporary and persistent cookies is considered to be personal information and therefore subject to PIPEDA. The OPC has adopted the same position with respect to information collected in connection with online behavioral advertising;

In Privacy and Online Behavioral Advertising, the OPC stated that it may be permissible to use opt-out consent in the context of online behavioral advertising if the following conditions are met:

- Individuals are made aware of the purposes for the online behavioral advertising, at or before the time of collection, in a manner that is clear and understandable
- Individuals are informed of the various parties involved in the online behavioral advertising at or before the time of collection
- Individuals are able to opt-out of the practice and the opt-out takes effect immediately and is persistent
- The information collected is non-sensitive in nature (ie, not health or financial information), and
- The information is destroyed or made de-identifiable as soon as possible

The OPC has indicated that online behavioral advertising must not be a condition of service and, as a best practice, should not be used on websites directed at children.

Canadian privacy regulatory authorities also consider location data, whether tied to a static location or a mobile device, to be personal information. As such, any collection, use or disclosure of location data requires, among other things, appropriate notice, and consent. Most of the privacy regulatory authority decisions related to location data have arisen with respect to the use of GPS in the employment context.

The Canadian privacy regulatory authorities provide the following test that must be met for the collection of GPS data (and other types of monitoring and surveillance activities):

- Is the data demonstrably necessary to meet a specific need?
- Will the data likely be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Are there less privacy-intrusive alternatives to achieve the same objective?

Bill 64 introduced several changes to the Quebec Private Sector Act which significantly impact online privacy. Starting September 22, 2023, organizations collecting personal information by offering a product or service with privacy parameters must ensure that the highest privacy settings are enabled by default. Additionally, organizations collecting personal information from persons using tracking, localization or profiling technology (including cookies, trackers, and similar technologies) have the obligation to inform the person in advance of the use of such technologies, and to inform the person of the method for activating such functions: the use of such technologies therefore requires opt-in consent. Profiling is broadly defined as the collection and use of personal information in order to evaluate certain characteristics of a person such as workplace performance, economic or financial situation, health, personal preferences or interest, or behaviour.

Artificial Intelligence

The OPC has also issued guidance on the appropriate use of generative AI systems and has stated that generative AI systems should be developed with the general principles of legality, appropriate purposes, necessity and proportionality, openness and accountability, and:

- In a manner that allows individuals to meaningfully exercise their rights to access their personal information; while
- limiting collection, use and disclosure to only what is needed to fulfill the identified purpose; and
- implementing appropriate safeguards

In addition, the OPC has stated that developers of generative AI models should take steps to ensure that outputs should be as accurate as possible.

KEY CONTACTS



Tamara Nielsen
Counsel
T +1 604.643.2952
tamara.nielsen@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.