

## COMPARATIVE TABLE BETWEEN BILL 64 (QUEBEC) AND BILL C-11 (CANADA)

Fasken's Privacy and Cybersecurity Practice Group  
William Deneault-Rouillard

FASKEN

National group leaders : Antoine Aylwin and Alex Cameron  
Strategic advisor : Jennifer Stoddart<sup>1</sup>

		QUEBEC	CANADA
		<i>Act respecting the protection of personal information in the private sector amended by Bill 64, An Act to modernize legislative provisions as regards the protection of personal information</i>	<i>Bill C-11, An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts</i>
1.	Last stage completed in the legislative process	Passage in principle on October 20, 2020.	First Reading in the House of Common on November 17, 2020.
2.	Responsible authority	Commission d'accès à l'information (CAI)	Office of the Privacy Commissioner of Canada (OPC) Data Protection Tribunal
3.	Scope of application	<ul style="list-style-type: none"> <li>Any "enterprise" (within the meaning of the <i>Civil Code of Québec</i>) which collects, holds, uses or communicates personal information whether it keeps the information itself or through a third person.</li> </ul> <p>Applies to personal information held by a professional order to the extent provided for by the <i>Professional Code</i> and to that held by an authorized entity to the extent provided for by the Election Act (chapter E-3.3).</p> <ul style="list-style-type: none"> <li>Excluding public bodies within the meaning of the Act respecting Access to documents held by public bodies and the Protection of personal information (CQLR, c. A-2.1)</li> </ul>	<p>Applies to every organization in respect of personal information that</p> <ul style="list-style-type: none"> <li>the organization collects, uses or discloses in the course of commercial activities; or</li> <li>is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.</li> </ul> <p>The Act applies in respect of personal information</p> <ul style="list-style-type: none"> <li>that is collected, used or disclosed interprovincially or internationally by an organization; or</li> </ul>

<sup>1</sup> Counsel in Fasken's National Privacy and Cybersecurity Practice Group. This document is not intended to be exhaustive and does not constitute legal advice. This document was last updated on December 10, 2020.

		QUEBEC	CANADA
			<ul style="list-style-type: none"> <li>• that is collected, used or disclosed by an organization within a province, to the extent that the organization is not exempt from the application of this Act under an order made under paragraph 119(2)(b)</li> <li>• The Act also applies to service providers, they are exempt from obligations except for safeguards and breach notification.</li> </ul>
4.	<b>Personal information</b>	<ul style="list-style-type: none"> <li>• Any information which relates to a natural person and allows that person to be identified (s. 2).</li> <li>• Whatever the nature of its medium and whatever the form (written, graphic, taped, filmed, computerized, or other) (s. 1)</li> </ul> <p>Does not apply to personal information that is public by law or concerning the performance of duties within an enterprise by the person concerned, such as the person's name, title and duties, as well as the address, email address and telephone number of the person's place of work (s. 1).</p>	Means information about an identifiable individual (s 2, Definitions)
5.	<b>Sensitive information</b>	<ul style="list-style-type: none"> <li>• Definition : personal information is sensitive if, due to its nature or the context of its use or communication, it entails a high level of reasonable expectation of privacy (s. 12).</li> <li>• Consent must be given expressly when it concerns sensitive personal information (s. 12 and 13)</li> </ul>	<p>No definition but :</p> <p>An organization that de-identifies personal information must ensure that any technical and administrative measure applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information (s. 74);</p> <p>An organization may choose to give an individual access to sensitive medical information through a medical practitioner (s. 66 (3));</p> <p>The sensitivity of the personal information involved in a security breach is a factor in assessing the real risk of significant harm (s. 58 (ss8) (3));</p> <p>The level of protection provided by security safeguards must be proportionate to the sensitivity of the information (s57 (1));</p> <p>The sensitivity of the personal information is a factor to be taken into account in determining whether the purpose for which it is used collected and disclosed is appropriate (s12(2)(a))</p>

		QUEBEC	CANADA
6.	<b>Consent</b>	<ul style="list-style-type: none"> <li>• Must be clear, free and informed and be given for specific purposes. It must be requested for each such purpose, in clear and simple language and separately from any other information provided to the person concerned. If the person concerned so requests, assistance is provided to help him understand the scope of the consent requested (s. 14)</li> <li>• Such consent is valid only for the length of time needed to achieve the purposes for which it was requested (s. 14)</li> <li>• Consent withdrawal is possible (s. 8 and 22)</li> <li>• Not required when an exception applies, notably:               <ul style="list-style-type: none"> <li>• personal information is used for purposes consistent with those for which it was collected,</li> <li>• when its use is clearly for the benefit of the individual concerned, and</li> <li>• when it is de-identified and its use is necessary for study, research or statistical purposes (s. 12).</li> </ul> </li> </ul>	<p>An organization developing a privacy management program must take into account the volume and sensitivity of the personal information under its control (s 9(2))</p> <ul style="list-style-type: none"> <li>• Presumption of express consent</li> <li>• Exclusion to consent requirements for transfers to service providers do not require consent.</li> <li>• Individual consent must be obtained before the time of the collection of PI. The individual consent is valid only if it is provided with information regarding the purpose of the collection, the way in which the PI is to be collected, used or disclosed, any foreseeable consequences, the specific type of PI that is to be collected, used or disclosed and the names of any third parties to which the organization may disclose the PI. (s. 15)</li> <li>• The consent must be express unless the organization establishes it is appropriate to rely on implied consent (s. 15(4))</li> <li>• Individuals can withdraw their consent (art.17)</li> <li>• Consent not required when an exception applies, notably (art.18-51 state the exceptions) :               <ul style="list-style-type: none"> <li>○ Carrying out a business activity such as providing a product or service requested by the individual, securing an organization's information, systems or networks, or where it is virtually impossible to obtain the individual's consent due to the lack of a direct relationship with the individual (s. 18 (1));</li> <li>○ Transfer personal information to service providers (s. 19 );</li> <li>○ De-identify personal information (s. 20);</li> <li>○ Use de-identified information for internal research and development purposes (s. 21).</li> </ul> </li> </ul>
7.	<b>Impact Assessments</b>	<p>Obligation for enterprises to conduct an assessment of the privacy-related factors (privacy impact assessment) of any information system project involving the collection, use, disclosure, retention or destruction of personal information (s. 3.3).</p>	<p>Organizations to implement a "privacy management program" that can be reviewed and even certified by the OPC (ss. 9, 10 and 77)</p>

		QUEBEC	CANADA
8.	<b>Children</b>	<ul style="list-style-type: none"> <li>Consent must be given by the person who has the parental authority for information concerning a minor under 14 years of age, unless the information is clearly for the minor's benefit (s. 4.1 and 14)</li> <li>Section 38 pertaining to information of a medical or social nature (but subject to the general rules of the Civil Code of Québec)</li> </ul>	No specific regime for minors or children, but the rights and remedies provided by law may be exercised on behalf of the minor or any other incapacitated person by the person authorized by law to manage his or her affairs or property (art. 4).
9.	<b>Right of access</b>	<ul style="list-style-type: none"> <li>Yes, subject to certain exceptions, including in the event of litigation or if it may seriously harm a third person (s. 40)</li> <li>Written request for access with proof of identity (s. 30)</li> <li>Response within 30 days (s. 32)</li> <li>Free of charge (a reasonable charge may be required in certain conditions, s. 33)</li> <li>The enterprise has an obligation to provide assistance to ensure that concerned individuals have access to their personal information.</li> </ul>	<ul style="list-style-type: none"> <li>Yes, upon request by an individual, an organization must inform them of whether it has any personal information about them, how it uses the information and whether it has disclosed the information. It must also give the individual access to the information (art. 63(1))</li> <li>Written request (art. 64(1))</li> <li>Response within 30 days (art. 67(1))</li> <li>Free of charge unless the conditions are fulfilled (art.68)</li> <li>Organization must assist the individual (art.64(2))</li> </ul>
10.	<b>Right to correct (or to rectify)</b>	<ul style="list-style-type: none"> <li>Yes, if the information is inaccurate or incomplete (s. 28)</li> <li>Rights of access requirements apply with the necessary changes (s. 30 and following)</li> </ul>	<ul style="list-style-type: none"> <li>Not explicitly stated as a right to correct/rectify, but: An organization must take reasonable steps to ensure that personal information under its control is as accurate, up-to-date and complete as is necessary to fulfil the purposes for which the information is collected, used or disclosed (Art. 56(1))</li> </ul>
11.	<b>Right to erasure</b>	<ul style="list-style-type: none"> <li>No, but where the purposes for which personal information was collected or used are achieved, the person carrying on an enterprise must destroy or anonymize the information, subject to any preservation period provided for by an Act (s. 23)</li> </ul> <p>Individuals have the right to require that such information cease to be disseminated or that any hyperlink attached to the person's name providing access to the information by a technological means be de-indexed or re-indexed.</p>	<ul style="list-style-type: none"> <li>Partial right of erasure: As soon as feasible upon the receipt of the individual's written request, unless the disposal would result in the disposal of personal information about another individual or requirements of the Act or a contract prevent it. The individual must be informed in writing of the refusal to dispose of their personal information (art. 55) .</li> </ul> <p>The organization must also inform any service provider to whom it has transferred personal information and obtain a confirmation that the information has been disposed of (art.55(3)).</p>

		QUEBEC	CANADA
12.	<b>Right to portability</b>	Yes, right to obtain copy of personal information held by an enterprise in a structured commonly used technological format upon request or communicated to an authorized person or body. (s112)	Regulations will provide a data mobility framework in order to allow a subject organization, upon request, to disclose personal information to another subject organization (art. 72), However, no right for the concerned individual to obtain the personal information in such format.
13.	<b>Automated decision</b>	<p>Specific regime applicable to decisions based exclusively on automated processing (s. 12.1).</p> <p>Right to know about the personal information, the reasons, factors and parameters used to make the decision and to have the information corrected Right to submit observations for review.</p>	<p>Automated decision system means any technology that assists or replaces the judgement of human decision-makers (s. 2).</p> <p>If the organization has used an automated decision system to make a prediction, recommendation or decision about the individual, the organization must, on request by the individual, provide them with an explanation of the prediction, recommendation or decision and of how the personal information that was used to make the prediction, recommendation or decision was obtained. (s. 63)</p>
14.	<b>Right to redress</b>	<ul style="list-style-type: none"> <li>Right to submit an application to the CAI for the examination of a disagreement (s. 42 and following)</li> </ul>	Written complaint to Privacy Commissioner (s82(1) and following)
15	<b>De-identification</b>	<ul style="list-style-type: none"> <li>Personal information is depersonalized when it no longer allows the direct identification of the person concerned (s. 12 (4)). This information remains subject to the legislation considering that it is always possible to identify an individual from depersonalized information.</li> <li>Only "anonymized" information, i.e. information that no longer allows the direct or indirect identification of a natural person (s. 23 (2)), is not subject to the restrictions of the Act. Anonymization must be done in accordance with the industry best practices.</li> <li>Penal provisions and fines for persons who make or attempt to make an identification of an individual based on de-identified information (s. 91).</li> </ul>	<p>No distinction between depersonalization and anonymization. The act of "de-identifying" is defined as modifying personal information - or creating information from personal information - through technical processes so that the information is not personally identifiable and cannot, under reasonably foreseeable circumstances, be used, either alone or in combination with other information, to identify an individual (s. 2).</p> <ul style="list-style-type: none"> <li>An organization may use personal information without consent to de-identify it (s. 20).</li> <li>The technical and administrative procedures used to de-identify personal information must be proportionate to the purposes for which the information is being de-identified and the sensitivity of the personal information (s. 74).</li> <li>Except for the purpose of verifying the effectiveness of the security measures in place, no organization shall use de-identified information, alone or in combination with other information, to identify an individual (s. 75).</li> </ul>
16.	<b>Person in charge and governance</b>	<ul style="list-style-type: none"> <li>Yes, the "person in charge of the protection of personal information" (s. 3.1)</li> </ul>	<ul style="list-style-type: none"> <li>An organization must designate one or more individuals to be responsible for matters related to its obligations under this Act. It must provide the designated individual's business contact information to any person who requests it.</li> </ul>

		QUEBEC	CANADA
		<ul style="list-style-type: none"> <li>• He must establish and implement governance policies and conduct assessment of the privacy-related factors of any project or system involving PI (s. 3.2 and 3.3.)</li> <li>• Has a role of report to the Commission d'accès à l'information in case of a confidentiality incident of high risk (s. 3.5).</li> <li>• Has a role in access and rectification demands of individuals who have PI owned by its enterprise (s. 30).</li> </ul>	<ul style="list-style-type: none"> <li>• Every organization must implement a privacy management program that includes the organization's policies, practices and procedures (s. 9)</li> </ul>
17.	<b>Obligations of transparency</b>	<ul style="list-style-type: none"> <li>• Inform the individual concerned of the object of the file, the use which will be made of the information and the categories of persons who will have access to it within the enterprise, and the place where the file will be kept and of the rights of access and rectification.</li> <li>• The company must inform in simple and clear terms the individuals concerned by the collection, in particular : <ul style="list-style-type: none"> <li>○ the purposes for which the information is being collected;</li> <li>○ the means by which the information is being collected;</li> <li>○ the rights of access and rectification provided by law;</li> <li>○ their right to withdraw their consent to the communication or use of the information collected;</li> <li>○ where appropriate, the person concerned is informed of the name of the third party for whom the information is being collected and of the possibility that the information may be disclosed outside Québec; and</li> <li>○ certain information and means relating to the use of a technology that includes functions allowing the identification, localization or profiling of individuals.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfil its obligations under this Act (s. 62)</li> <li>• In particular, the organization must make the following information accessible: <ul style="list-style-type: none"> <li>○ a description of the type of personal information under its control;</li> <li>○ a general explanation of the use to which the personal information is to be put, including how the organization applies the exceptions to the requirement to obtain an individual's consent set out in this Act;</li> <li>○ a general explanation of how the organization uses automated decision making systems to make predictions, recommendations or decisions that could have a significant impact on individuals; and</li> <li>○ whether or not it engages in interprovincial or international transfers or disclosures of personal information that may have a reasonably foreseeable impact on privacy.</li> <li>○ how to make a request for the withdrawal of personal information or a request for access to personal information;</li> <li>○ the business contact information of the individual to whom inquiries and complaints may be directed (s. 62).</li> </ul> </li> </ul>

		QUEBEC	CANADA
18.	<b>Security measures</b>	<ul style="list-style-type: none"> <li>Implement security measures necessary to ensure the protection of the personal information that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored (s. 10).</li> </ul>	<ul style="list-style-type: none"> <li>An organization must protect personal information through physical, organizational and technological security safeguards. The level of protection provided by those safeguards must be proportionate to the sensitivity of the information. In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, taking into account the quantity, distribution, format and method of storage of the information (s. 57).</li> <li>Security safeguards must protect personal information against, among other things, loss or theft and unauthorized access, disclosure, copying, use or modification (s. 57).</li> <li>The technical and administrative measures applied to the information must be proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information (s. 74 and 75).</li> </ul>
19.	<b>Breach notification</b>	<ul style="list-style-type: none"> <li>If the breach presents a risk of serious injury, a notification to the Commission d'accès à l'information and to concerned individuals must be made (s. 3.5).</li> <li>However, a person whose personal information is concerned by the incident need not be notified so long as doing so could hamper an investigation conducted by a person or body responsible by law for the prevention, detection or repression of crime or statutory offences (s. 3.5).</li> </ul>	<ul style="list-style-type: none"> <li>If the breach of security safeguards presents a real risk of significant harm to the individual, a report must be given to the Commissioner (art.58(1))</li> <li>Unless otherwise prohibited by law, an organization must notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual (art.57(3))</li> </ul>
20.	<b>Transfer to foreign jurisdictions</b>	<ul style="list-style-type: none"> <li>Before transferring information outside of Quebec, an assessment of privacy-related factors must be made (s. 17).</li> <li>The transfer can be done if the assessment establishes and equivalent protection to the one afforded under the Quebec's Act (s. 17).</li> <li>The transfer must be subject of a written agreement (S. 17).</li> <li>A list of States offering equivalent protection could be published by government (s. 17).</li> <li>Theses conditions don't apply if the transfer is made by reason of the urgency of a situation that threatens the life, health or safety of the person concerned (s. 18(7) and 17).</li> </ul>	<ul style="list-style-type: none"> <li>Transfer to service providers can be done without the individual's knowledge or consent (S. 19)</li> <li>Transfer to service providers, the organization must ensure, by a contract, that the service provider provides substantially the same protection for the personal information (s. 11)</li> </ul>

		QUEBEC	CANADA
21.	<b>Other obligations and provisions</b>	Privacy by default.	
22.	<b>Retention of information</b>	<ul style="list-style-type: none"> <li>For such time as is necessary for the purposes identified or to allow the individual concerned to exhaust the recourses provided by law (s. 23).</li> <li>Ensure that any file held on another individual is up to date and accurate when used by an enterprise to make a decision in relation to the individual concerned. The information used to make such a decision is kept for at least one year (s. 11)</li> <li>No retention schedule established by government regulation.</li> </ul>	<ul style="list-style-type: none"> <li>Information is retained for as long as required to fulfill the purposes for which the information was collected, used or disclosed, or to fulfill legal requirements (art. 53).</li> <li>An organization that uses personal information to make a decision about an individual must retain the information for a sufficient period of time to permit the individual to make a request for access.</li> <li>No retention schedule established in the law.</li> </ul>
23.	<b>Statutory penalties</b>	<ul style="list-style-type: none"> <li>\$5,000 to \$50,000 for a contravention of the provisions of the Act in case of a natural person (S. 91)</li> <li>\$15,000 to \$25,000 for a contravention of the provisions of the Act in all other case (s. 91)</li> <li>4 % of the worldwide turnover for the preceding fiscal year (s. 91)</li> <li>Penalties for subsequent offences are doubled (s. 92.1)</li> </ul>	<ul style="list-style-type: none"> <li>Possibility of the Commissioner entering into compliance agreements with the organization (art. 86)</li> <li>The Commissioner can make a recommendation for a penalty if he finds, after an inquiry, that an organization does not comply with the Act (s. 93)</li> <li>Penalties cannot be given for an organization that establishes that it exercised due diligence to prevent the contravention (s. 94)</li> <li>In determining whether or not a penalty is appropriate, and determining the amount of a penalty, the tribunal must take some factors into account (s. 94): <ul style="list-style-type: none"> <li>the nature and scope of the contravention;</li> <li>whether the organization has voluntarily paid compensation to a person affected by the contravention;</li> <li>the organization's history of compliance with this Act; and</li> <li>any other relevant factor.</li> </ul> </li> <li>The organization can be guilty of an indictable offence for contravention of certain sections of the Act or interfering with the Commissioner's investigation, inquiry or audit.</li> <li>Indictable offence and liable to a maximal fine of \$25M or 5 % or the organization's gross global revenue for the preceding financial year;</li> </ul>

		QUEBEC	CANADA
			<ul style="list-style-type: none"><li>• Guilty or a summary conviction offence and liable to a fine not exceeding the higher of \$20M or 4 % or the organization's gross global revenue for the preceding financial year.</li></ul>
24.	<b>Other remedies for the individual</b>	<ul style="list-style-type: none"><li>• Remedies available from the CAI</li><li>• Remedies available from the courts (including by way of a class action)</li><li>• Punitive damages if the infringement of the Act is intentional or results from a gross fault (s. 93.1)</li></ul>	Individual has a private right of action against an organization for damages for loss or injury if the Commissioner has made a finding of contravention of the Act which is not appealed or the Tribunal has made such a finding or the organization has been convicted of an offence. The individual has two years from such a finding decision or conviction to appeal to the Federal Court or a superior court of a province (art. 106).