

# Personal Information Protection by Companies Conducting Business in Quebec: Adoption of Bill 64

Vanessa Coiteux, Geneviève Paradis, Catherine Jenner, Danielle Miller Olofsson

## How will the Reform affect companies' privacy practices?

On September 21, 2021, the National Assembly adopted Bill 64, an [Act to modernize legislative provisions as regards the protection of personal information](#) (the “**Act**”). This new Act introduces significant changes to the protection of personal information in the private and public sectors in Quebec (the “**Reform**”).

We have summarized below the important provisions of this Act that will affect companies doing business in Quebec. These new requirements and sanctions, that take effect progressively on September 22, 2022, September 22, 2023 or September 22, 2024, target three areas in particular: governance, operations, and data subject rights.

## What are the main differences between the Act and PIPEDA?

Since some Quebec businesses are also subject to the [Personal Information Protection and Electronic Documents Act \(Canada\)](#) (“**PIPEDA**”), we have set out below the differences between certain provisions introduced by the Act and the requirements currently provided for in PIPEDA.

Several of the Act’s amendments resemble PIPEDA provisions. The first example of this is the business transaction exception allowing for the communication of personal information in the context of a commercial transaction without the prior consent of the data subject. This amendment is long awaited by the Quebec business community as it greatly facilitates the transactional process. Also of note, information concerning a person’s professional function such as their name, title, function and professional email, address, and telephone number, will no longer be subject to the requirements of the Act.

## I. Main Features

Provision	New Requirements	Notable Differences with PIPEDA	Practical Application	Effective Date
<b>Governance</b>				
<b>Appointment of a Privacy Officer (s. 3.1)</b>	<ul style="list-style-type: none"> <li>The Reform requires every business to appoint a Privacy Officer and to publish their name and contact details on its website.</li> <li>This function is attributed to the most senior officer of the company who is responsible for ensuring compliance and implementation of the Act. This function may be delegated to any person.</li> </ul>	<ul style="list-style-type: none"> <li><i>No significant difference</i>; PIPEDA requires that a responsible person be identified but does not assign statutory responsibility to the most senior officer.</li> </ul>	<ul style="list-style-type: none"> <li>We recommend the appointment of a person qualified in compliance and cyber security.</li> <li>Publication of the contact information of the person in charge on the business' website.</li> </ul>	September 22, 2022
<b>Policies, practices and transparency (ss. 3.2, 8 and 8.2)</b>	<ul style="list-style-type: none"> <li>Businesses must establish and implement personal information governance and protection policies and practices.</li> <li>These policies and practices are to be commensurate with the nature and importance of the business activities and are to be approved by the Privacy Officer.</li> </ul>	<ul style="list-style-type: none"> <li><i>No significant difference</i>; similar requirements to establish and maintain policies and practices regarding the management of personal information.</li> <li>But PIPEDA does not require disclosure of detailed information about a business' internal policies and practices with respect to the protection and/or management of personal information.</li> </ul>	<ul style="list-style-type: none"> <li>If not already in place, implement policies and practices to ensure the protection of personal information that include: (i) rules applicable to the retention and destruction of personal information; (ii) the roles and responsibilities of employees throughout the life cycle of personal information; and (iii) a complaint handling process.</li> <li>Publication of detailed information<sup>1</sup> on these policies and practices on the business' website.</li> </ul>	September 22, 2023

<sup>1</sup> The Act does not specify the scope of this disclosure.

Provision	New Requirements	Notable Differences with PIPEDA	Practical Application	Effective Date
<b>Operations</b>				
<b>Privacy Impact Assessment (ss. 3.3. and 3.4)</b>	<ul style="list-style-type: none"> <li>Businesses are required to conduct a Privacy Impact Assessment (“PIA”) of any information system acquisition, development, redesign or electronic service delivery project involving the collection, use, disclosure, retention or destruction of Personal Information.</li> </ul>	<ul style="list-style-type: none"> <li>There is no such requirement in PIPEDA.</li> </ul>	<ul style="list-style-type: none"> <li>Develop PIA template(s) of factors to consider.</li> <li>Ensure these factors include the ability to communicate information collected from a data subject to that data subject upon request in a commonly used and machine-readable format.</li> <li>Establish a policy for when a PIA is required (i.e., a project involving the management or processing of personal information or transfer outside of Quebec).</li> </ul>	September 22, 2023
<b>Privacy incident (ss. 3.5 to 3.8)</b>	<ul style="list-style-type: none"> <li>When a privacy incident<sup>2</sup> occurs that poses a risk of serious harm, businesses are required to notify the Commission d'accès à l'information (“CAI”) and the data subjects involved unless such notification would hinder an investigation.</li> <li>The assessment of the concept of risk of serious harm is based on the following factors: (i) the sensitivity of the information involved; (ii) the apprehended consequences of its use; and (iii) the likelihood that the information will be used for harmful purposes.</li> </ul>	<ul style="list-style-type: none"> <li><i>No significant difference</i>; similar requirements for notifying the Privacy Commissioner of Canada (the “Commissioner”) and the individuals involved.</li> </ul>	<ul style="list-style-type: none"> <li>If not already in place, implement a policy detailing the steps to take in the event of a privacy incident.</li> <li>Develop an incident response plan.</li> <li>Maintain a register of all privacy incidents which shall be made available to CAI upon request.</li> <li>Notification to CAI and affected persons as well as to any person that can help mitigate the damages.</li> </ul>	September 22, 2022

<sup>2</sup> The term “privacy incident” is defined as unauthorized access, use or disclosure, loss or other breach of personal information.

Provision	New Requirements	Notable Differences with PIPEDA	Practical Application	Effective Date
<b>Consent (ss. 8.1, 8.3, 12 and 14)</b>	<ul style="list-style-type: none"> <li><i>Implied Consent:</i> By providing personal information, an individual consents to the collection, use and disclosure of his or her personal information for the purposes identified in this policy.</li> <li><i>Express consent:</i> when consent is required under the Act, it must be clear, free, informed and provided for a specific purpose.</li> <li>Businesses must obtain express consent for sensitive personal information. Information is considered sensitive when, because of its medical, biometric, or other intimate nature, or because of the context of its use or disclosure, it gives rise to a high level of reasonable expectation of privacy.</li> </ul>	<ul style="list-style-type: none"> <li><i>No significant difference;</i> similar requirements for type of consent depending on sensitivity of personal information.</li> </ul>	<ul style="list-style-type: none"> <li>Publication of a privacy policy on the business' website that sets out: (i) the purposes for which personal information is collected, used, retained and disclosed; (ii) the means by which it is collected; (iii) the implied consent of users to the purposes and means detailed in the policy; (iv) the rights of access and rectification provided by the Act; and (v) the right of an individual to withdraw consent.</li> <li>If technology used to collect personal information allows for identification, location or profiling, the data subject must be informed of: i) the use of such technology; and ii) any means of de-activating it.</li> <li>Establishment of a control process for obtaining express consent for the collection, use, retention and disclosure of sensitive personal information.</li> </ul>	September 22, 2023
<b>Privacy settings (s. 9.1)</b> <b>«Privacy by Design »</b>	<ul style="list-style-type: none"> <li>The Act requires that the privacy settings of any technology product or service provided by a business that collects personal information offer the highest level of privacy by default.</li> <li>This does not apply to cookies.</li> </ul>	<ul style="list-style-type: none"> <li>PIPEDA does not have such a requirement but provides that any use of cookies must be disclosed in the company's privacy policy.</li> </ul>	<ul style="list-style-type: none"> <li>The company's website configuration ensures robust privacy settings by default.</li> </ul>	September 22, 2023
<b>Automated processing (s. 12.1)</b>	<ul style="list-style-type: none"> <li>Businesses that use personal information to make a decision based exclusively on automated processing shall inform the individual concerned.</li> </ul>	<ul style="list-style-type: none"> <li>There is no such requirement under PIPEDA.</li> </ul>	<ul style="list-style-type: none"> <li>We recommend that any business that bases its decision to offer a product or services exclusively on a automated analysis of a client's profile disclose this.</li> </ul>	September 22, 2023

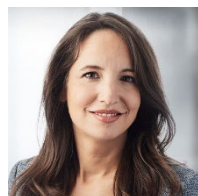
Provision	New Requirements	Notable Differences with PIPEDA	Practical Application	Effective Date
<b>Transfers outside Quebec (s. 17)</b>	<ul style="list-style-type: none"> <li>Before disclosing any personal information outside Quebec, each business must conduct a PIA.</li> <li>The results of the PIA should demonstrate that the personal information outsourced to a service provider in another jurisdiction will receive adequate protection.</li> <li>These requirements also apply to any business that engages a business outside Quebec to collect, use, communicate or store personal information on its behalf.</li> </ul>	<ul style="list-style-type: none"> <li>PIPEDA does not provide for such a requirement, but it does provide that any company that discloses personal information outside of Canada remains responsible for protecting the confidentiality of the personal information disclosed and must inform the individuals involved.</li> </ul>	<ul style="list-style-type: none"> <li>In this instance the PIA should consider the following factors: (i) the sensitivity of the information; (ii) the purpose for which it is to be used; (iii) the safeguards in place; and (iv) the applicable legal regime of the jurisdiction where the information will be disclosed.</li> <li>A written agreement must be entered into between the business and the service provider.</li> </ul>	September 22, 2023
<b>Outsourcing (s. 18.3)</b>	<ul style="list-style-type: none"> <li>A business may, without the consent of the individual, send information to a service provider located in another jurisdiction on condition that a written agreement is in place.</li> </ul>	<ul style="list-style-type: none"> <li><i>No significant difference</i>; similar requirements for signing an outsourcing agreement.</li> </ul>	<ul style="list-style-type: none"> <li>Drafting of model clauses to be included in any outsourcing agreement outside Quebec that provide for: (i) the measures to be taken to ensure the protection of personal information; (ii) the purposes for which disclosure is permitted; and (iii) an undertaking to notify the company of any breach or attempted breach of the obligations relating to the confidentiality of the information disclosed.</li> </ul>	September 22, 2023
<b>Destruction or Anonymization (s. 23)</b>	<ul style="list-style-type: none"> <li>Once the purpose for which personal information was collected or used has been fulfilled, the company shall destroy or de-identify the information and use it for a meaningful and legitimate purpose.</li> </ul>	<ul style="list-style-type: none"> <li><i>No significant difference</i>; similar requirements for destruction of personal information once purposes have been fulfilled.</li> </ul>	<ul style="list-style-type: none"> <li>If not already in place, implement a policy for the retention of personal information and implement practices to ensure the destruction or de-identification of personal information in accordance with that policy.</li> </ul>	September 22, 2023

Provision	New Requirements	Notable Differences with PIPEDA	Practical Application	Effective Date
<b>Data Subject's Rights</b>				
<b>Right to portability (s. 27)</b>	<ul style="list-style-type: none"> <li>Any individual whose personal information has been collected by a business may request a written transcript of the computerized information.</li> <li>They may ask that the business communicate to them any personal information collected in a commonly used and machine-readable format</li> <li>However, this excludes information created or inferred by the business through an analysis of the individual's personal information.</li> </ul>	<ul style="list-style-type: none"> <li>PIPEDA does not provide a similar right but does provide a general right of access to personal information collected by a business.</li> </ul>	<ul style="list-style-type: none"> <li>Implementation of practices that facilitate access to all personal information that a business holds about an individual and allow for its complete transcription into a structured and commonly used technological format.</li> </ul>	September 22, 2024
<b>Right to de-indexation (s. 28.1)</b>	<ul style="list-style-type: none"> <li>An individual may request that a business de-index or cease the release of his or her personal information if the release contravenes the Act or a court order or if certain conditions are met including (i) the dissemination causes serious harm to the individual's reputation or privacy; (ii) the harm clearly outweighs the public's interest in knowing the information or any individual's interest in free speech; and (iii) the request to cease dissemination does not exceed what is necessary to prevent the harm.</li> </ul>	<ul style="list-style-type: none"> <li>PIPEDA does not provide for any such right.</li> </ul>	<ul style="list-style-type: none"> <li>Implementation of practices that facilitate the de-indexation of all personal information that a company holds on an individual.</li> </ul>	September 22, 2023

## II. New Penalties introduced by the Reform

	New Penalties	PIPEDA	Effective Date
<b>Administrative Monetary Penalties (s. 90.1 and ss. 90.12 and 91)</b>	<ul style="list-style-type: none"> <li>The Act grants the CAI the power to impose: (i) administrative penalties of up to \$10,000,000 or 2% of the company's worldwide turnover and (ii) criminal penalties of up to \$25,000,000 or 4% of the company's worldwide turnover.</li> <li>Grounds under which the CAI could impose a sanction include, but are not limited to: (i) collecting, disclosing, using or destroying personal information in violation of the law; (ii) failing to report a privacy incident; (iii) failing to have a privacy policy that complies with prescribed requirements; or (iv) having deficient security measures to ensure the protection of personal information.</li> </ul>	<ul style="list-style-type: none"> <li>Under PIPEDA, the Commissioner does not have the power to impose administrative or criminal sanctions. The Commissioner may initiate a complaint, investigate complaints, conduct audits and initiate legal proceedings in federal court.</li> <li>The grounds on which the federal court could order a company to pay damages to the complainant are similar to those set out in the Act, however the amount of damages that can be awarded is significantly lower, namely: (i) a minimum penalty of \$10,000 and (ii) a maximum penalty of no more than \$100,000.</li> </ul>	September 22, 2023
<b>Private right of action (s. 93.1)</b>	<ul style="list-style-type: none"> <li>Finally, the Act introduces a private right of action for individuals who suffer harm as a result of an unlawful infringement of a right conferred by the Act or of certain articles of the <i>Civil Code of Québec</i> relating to reputation and privacy.</li> <li>In addition, if the infringement is intentional or grossly negligent, the Act provides for punitive damages of at least \$1,000.</li> </ul>	<ul style="list-style-type: none"> <li>PIPEDA does not provide for a similar private right of action. The Commissioner may refer the complaint received to the Attorney General of Canada or of a province, as the case may be. The authority to which the complaint is referred may take action against the offender. Recent case law indicates that the damages awarded have generally been minimal.</li> </ul>	September 22, 2023

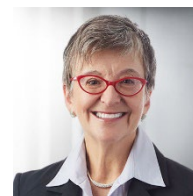
For further information, please contact your Stikeman Elliott representative or any of the following members of our Corporate Group:



**Vanessa Coiteux**  
Partner  
+1 514 397 3681  
[vcoiteux@stikeman.com](mailto:vcoiteux@stikeman.com)



**Geneviève Paradis**  
Senior Associate  
+1 514 397 3330  
[gparadis@stikeman.com](mailto:gparadis@stikeman.com)



**Catherine Jenner**  
Associate  
+1 514 397 3356  
[cjenner@stikeman.com](mailto:cjenner@stikeman.com)



**Danielle Miller Olofsson**  
Associate  
+1 514 397 3668  
[dmillerolofsson@stikeman.com](mailto:dmillerolofsson@stikeman.com)