JUNE 19, 2020 • 1 MIN READ

Québec's Bill 64 proposes sweeping changes to its privacy regime

AUTHORS

 Molly Reynolds

 Ronak Shah

 Teresa A. Reguly

La version française de cette communication est publiée ici.

On June 12, 2020, the Québec government introduced Bill 64 - *An Act to modernize legislative provisions as regards the protection of personal information*. Bill 64's objective "is to modernize the framework of personal information" in Québec to align with the digital context in which personal information is now used, and to provide citizens with "full control over their personal information".

What you need to know

Bill 64 introduces:

- European-style privacy obligations for both the public and private sector. The bill also proposes to regulate political parties.
- A mandatory breach notification requirement in line with existing federal requirements.
- Enhanced enforcement powers for the *Commission d'accès à l'information*, including prosecuting organizations for penal fines of up to $25 million or 4% of the organization's worldwide turnover and imposing monetary administrative penalties of up to $10 million or 2% of the organization's worldwide turnover.
- New data subject rights, including rights in relation to automated decision making and profiling, data portability rights and the right to be forgotten.

Overview of Bill 64's proposed amendments

The chart below summarizes the key features of the proposed Québec bill, and considers how the proposals align with existing federal privacy requirements. Those features that depart significantly from PIPEDA requirements will be of particular interest to organizations and industries that operate across Canada, as they may trigger significant compliance program changes or in-depth analysis of whether the Québec law binds them.

Key Feature Summary	Alignment with PIPEDA	Private Sector	Public Sector
Consent. Bill 64 proposes more onerous consent requirements. In particular, consent "must be requested for each [specific] purpose, in clear and simple language and **separately from any other information provided to the person concerned**." Further, the bill **requires express consent with respect to "sensitive"** personal information. Information is considered "sensitive" if, due to its nature or the context of its use or communication, it entails a high level of reasonable expectation of privacy. For minors under 14 years of age consent must be obtained from the person having parental authority.	The proposal to separate consent for each purpose from other terms significantly departs from PIPEDA. The expectation of express consent for sensitive information and parental consent for minors is consistent with existing interpretations and practice under PIPEDA, although drafted more explicitly.	✓	✓
Service provider exemption. Organizations may, without the consent of individual, disclose information to a third party "if the information is necessary for carrying out a mandate or performing a contract of enterprise or for services" as long as the mandate is in writing and a written agreement outlines accountability measures around the personal information that is shared, including a description of the service provider's safeguards and an obligation on the service provider to notify the controlling organization's privacy officer of actual or attempted confidentiality violations.	This aligns with PIPEDA, although the federal regulator has recently pushed against service provider sharing without consent.	✓	✓[1]
Business transaction exemption. Organizations may share information without prior consent for the purpose of carrying out a commercial transaction.	This is similar to PIPEDA's business transaction exemption.	✓	N/A

Secondary purposes and internal analytics exemptions. Organizations may use personal information without prior consent for:
• **Secondary purposes.** The bill introduces a secondary purpose exemption, which enables organizations to use personal information for a secondary purpose, as long as:
  • The use is for purposes consistent (i.e., direct and relevant) with the purposes for which it was collected[2]; or
  • It is used clearly for the benefit of the person concerned.
• **Internal Research and Analytics.** This exemption allows organizations to use personal information without prior consent as long as use is necessary for internal research or production of statistics, and the information is de-identified.
	There is no analogous exemption under PIPEDA[3].	✓	✓

Professional contact information exclusion. The bill introduces a full exclusion for professional contact information, defined as "personal information 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".	This is more generous than PIPEDA, which excludes business contact information only when used to communicate with an individual for business purposes.	✓	✓
Mandatory privacy impact analysis. Under the bill, organizations are required to conduct privacy impact assessments of any information system or electronic services delivery project that involves personal information.	This is not a PIPEDA requirement, but has long been required of federal public sector agencies.	✓[4]	✓
Cross-border adequacy and accountability requirements. Bill 64 requires organizations to conduct an assessment of privacy-related factors prior to transferring or disclosing any personal information outside Québec. Further, Bill 64 requires that information may only be communicated outside of Québec if: • the organization's assessment establishes that it would receive the same level of protection as afforded under Québec's privacy laws[5]; and • the organization enters into a written agreement with the entity to which the information is disclosed or transferred to ensure accountability.	PIPEDA contains no rules prohibiting cross-border personal information transfers. When transferring personal information cross border, the organization that transfers the personal information remains accountable. Post the OPC's *Equifax* findings and consultations on cross-border transfers, OPC requires organizations to be able to "demonstrate accountability", including through contractual means similar to those outlined in Bill 64. However, PIPEDA does not contain an adequacy requirement.	✓	✓
Mandatory breach notification and record keeping. Under Bill 64, organizations will be required to notify the Commission and impacted individuals, and may notify any relevant third-party, if the organization believes there is a "confidentiality incident" involving personal information that presents a "risk of serious injury"[6]. Organizations would also be required to maintain a register of confidentiality incidents.	This requirement in line with PIPEDA's breach notification. Interestingly, the bill does not require breach notification within 72 hours (as required under GDPR) but "promptly". Further unlike PIPEDA's requirement to keep records for a minimum of 2 years, there is no minimum prescribed period under the bill.	✓	✓

New monetary administrative penalties. Through this new procedure, the Commission would be required to issue a notice urging the organization to remedy a breach without delay and provide it with the opportunity to submit observations and documents. Thereafter, Bill 64 provides the Commission with the ability to impose **monetary administrative penalties of up to $10,000,000 or, if greater, the amount corresponding to 2% of the organization's worldwide turnover** for a variety of contraventions, including for failure to report a breach, processing of personal information in contravention of the Québec private sector privacy act, and failure to inform individuals about automated processing. Such fines would be subject to review by the Commission's oversight division and further review before the Court of Québec.	The OPC currently does not have such enforcement powers.	✓	✗
Penal regime. The bill proposes a penal regime whereby any organization that: • Collects, holds, communicates to third parties or uses personal information in contravention of the Act, • Fail's to report a breach, • Attempts to re-identify an individual without authorization where their information is de-identified, • Impedes the Commission's investigation, • Fails to comply with an order of the Commission Commits an offence and is liable to a **fine of: $15,000 to $25,000,000**, or, if greater, the amount corresponding to **4% of the organization's worldwide turnover** for the preceding year. Currently, only the Attorney General of Québec can institute penal proceedings for breaches of the act and fines are, in most circumstances, limited to a maximum of $10,000 for a first offence.	Fines under PIPEDA are more limited in scope and quantum. Under PIPEDA, failure to comply with the breach notification provisions is an offence and organizations may be liable for fines up to $100,000.	✓	✗
Penal regime for public sector organizations. The Commission can impose two tiers of fines, as part of a finding of a penal offence: • Between $3,000 and $30,000; or • Between $15,000 and $150,000.	Under the federal *Privacy Act* the maximum penalty fine is a $1000.	✗	✓

Private right of action. Bill 64 introduces: • statutory damages for "injury resulting from the unlawful infringement of a right" under the Québec private or public sector privacy acts, unless it results from superior force (i.e. force majeure). In addition, private sector organizations may be liable pursuant to the *Civil code of Québec*[7]; and • statutory punitive damages of at least $1000 where the infringement is "intentional or results from a gross fault". Accordingly, organizations may face increased exposure to privacy-related claims, including claims for punitive damages, and increased class action risks if Bill 64 is adopted as drafted.	Under PIPEDA, individuals can apply to the Federal Court after receiving the OPC's report or notice that an investigation is discontinued. The Federal Court, on a *de novo* review, can award damages. However, there are no statutory punitive damages under PIPEDA.	✓	✓
Increased director liability. Currently, Québec's private sector privacy act provides that directors and representatives of an organization who ordered, authorized, or consented to an offence, are liable for a penalty under the penal provisions. While this would remain the case, under Bill 64, directors would bear the risk of liability for substantially increased fines.	Directors may be found guilty of an offence and fined up to $100,000 if they knowingly fail to report breaches.	✓	N/A
Rights in relation to automated decision making. An organization that uses personal information to render a decision based exclusively on automated processing of the information must, at the time of or before the decision, inform the person concerned. On request, the organization must also inform the person of the personal information used to render the decision, the reasons, and the principal factors that led to the decision, and the person's right to correct the information. The organization would also be required to allow the person to submit observations for review of the decision.	PIPEDA currently does not provide data subjects such a right. The federal government is considering introducing such a right as part of its efforts to modernize PIPEDA (for more read our bulletin here).	✓	✓
Rights in relation to profiling. An organization that collects personal information using technology that has the ability to identify, locate or profile[8] the person whose information is collected must inform the individual of such technology and the means available, if any, to deactivate such technology.	PIPEDA currently does not provide data subjects such a right. The federal government is considering introducing such a right as part of its efforts to modernize PIPEDA.	✓	✓

Right to be forgotten. Bill 64 would require organizations to destroy or anonymize personal information when the purposes for which it was collected or used are achieved. Bill 64 would also provide individuals with the right to require organizations to cease disseminating personal information or to "de-index" any hyperlink attached to their name, that provides access to information by technological means, provided that conditions set forth in the Québec private sector privacy act are met.	The federal government's proposal to modernize PIPEDA has noted that the federal government, at this time, will not be considering the "right to be forgotten" because the matter is currently before the Federal Court.	✓	✗
Right to request source of information. Organizations that collect personal information from another person or organization, when requested, must inform the person of the source of the information.	PIPEDA does not provide for such a right.	✓	✗
Right to data portability. Under the current Québec public and private sector privacy acts, every organization that holds a file on another person must, at their request, confirm its existence and communicate to them any personal information that concerns them. Bill 64 would broaden this right by allowing the person to obtain a copy of the information in a written and intelligible transcript. The bill also allows individuals to request that organizations provide them with computerized personal information in a structured, commonly used technological format. The organization would also be required to release, at the individual's request, such information to any person or body authorized by law to collect such information.	PIPEDA currently does not provide data subjects such a right. The federal government is considering introducing such a right as part of its efforts to modernize PIPEDA.	✓	✓
Privacy by design. Bill 64 introduces a "privacy by design" approach that has been adopted under GDPR (Article 25). Bill 64 would require organizations that collect personal information when offering a technological product or service to ensure that the parameters provide the "highest level of confidentiality" by default, without intervention by the person concerned.	There is no such requirement under PIPEDA. However, the federal regulator has been pushing organizations to consider adopting a privacy by design philosophy.	✓	✗
Data protection officer. Organizations are required to designate a person "exercising the highest authority" who would be accountable for the organization's protection of personal information and to ensure that the organization complies with its statutory privacy law requirements.	This is similar to PIPEDA's stipulation to designate an individual who is accountable for its compliance with the Act, and to GDPR's requirement to designate a data protection officer under Article 37.	✓[9]	✓[10]

Heightened data governance. To enhance transparency, Bill 64 requires organizations to establish and implement governance policies and practices regarding personal information that ensure that must ensure the protection of the information. The bill requires organizations to establish and implement governance policies and practices regarding personal information. Additionally, organizations that collect personal information through technological means are obligated to publish a "confidentiality policy" on their website. The content and terms of such a policy will be determined by a government regulation.	This is in line with PIPEDA's openness and accountability requirements but goes further by prescribing that organizations publish those policies on their websites. There is no comparable requirement under PIPEDA to draft and publish a "confidentiality policy".	✓	✓

Bill 64 also introduces an amendment under the *Act to establish a legal framework for information technology,* which requires organizations to notify the Commission at least 60 days before a biometric database is brought into service[11]. This is a unique requirement that does not have parallels under federal or other provincial laws, and the new time-frame may add compliance and operational burdens to organizations that employ biometrics in customer service such as voiceprints, fingerprints, or gate analysis.

Conclusion

It is unlikely that the proposed amendments outlined in Bill 64 would come into effect prior to 2022. Bill 64 has been referred to the consultation stage at the Québec National Assembly, which is currently in recess and only comes back in September, and the transitional provisions provide that Bill 64 will come into force one year after the date of its assent. That said, organizations doing business in Québec should be prepared for significant changes to Québec's privacy landscape in the near future.

If passed, several of the amendments will make compliance with Québec's regime more onerous than complying with the federal regime. This means that organizations governed by PIPEDA that previously voluntarily complied with substantially similar provincial regimes may need to look more closely at the jurisdictional analysis. Many organizations will need to assess the risks, costs and benefits of either bringing their nationwide compliance program in line with the new Québec requirements, designing different protocols for Québec, or taking a firm stance that they are not subject to provincial laws and therefore do not need to depart from their existing data management program.

---

[1] The organization must provide the Commission with a copy of the written agreement. The agreement enters into force 30 days after it is received by the Commission.The bill also expands the exemption to meet 67.2 subparagraph 2's accountability measures to other public bodies who are performing the service provider contract.

[2] For the private sector act, the proposed amendment notes that commercial or philanthropic prospection are not considered "consistent purposes".

[3] PIPEDA requires organizations to notify individuals and obtain consent prior to using personal information for a new purpose not anticipated originally.

[4] This is novel, as federally only public sector entities are required to perform PIAs.

[5] The Minister will publish a list of jurisdictions whose legal framework is deemed to be equivalent to the personal information protection principles applicable in Québec in the *Gazette officielle du Québec*.

[6] Under Bill 64, failure to report a confidentiality incident to the Commission, or to the persons concerned, when required to do so is subject to both the monetary administrative penalties (up to $10 million) and penal fines (up to $25 million). This is significantly more than the maximum fine of $100,000 the Office of the Privacy Commissioner of

Canada can impose for failure to comply with the mandatory breach reporting requirements under PIPEDA.

[7] Articles 35 to 40 CCQ.

[8] Under Bill 64, "profiling" means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interests or behaviour.

[9] This person's information needs to be published on the organization's website or be made available by other means.

[10] For public bodies, the bill provides that they need to appoint a "committee on access to information and the protection of personal information is responsible for supporting the body in the exercise of its responsibilities and the performance of its obligations" under Quebec's public sector privacy act. The committee would be under the responsibility of the designated data protection officer.

[11] In the current act, organizations are required to disclose the existence of a biometric database to the Commission in advance, but no specific timeline is provided.

To discuss these issues, please contact the author(s).