

Bill 64 on modernizing Québec privacy law – Why it matters and how to prepare for it

September 23, 2021

Québec's Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, was adopted unanimously, on September 21, 2021, receiving assent on September 22, 2021. The clock has started running to prepare for its implementation in covered organizations. While most new provisions will come into effect only two years after assent, the organizational transformation they entail is significant and will require time and resources. To comply with Bill 64, organizations must: i) establish data governance processes, including ones to assist individuals in exercising new privacy rights, ii) develop corporate data management policies, iii) adopt technological solutions to de-index or transfer personal information upon request; and iv) issue internal guidelines to support staff and service providers in the implementation of the new privacy regime.

Bill 64 sets a precedent for important reform in Canadian private sector privacy law. Organizations should prepare for the changes it brings, even if they do not consider themselves governed by the Quebec law.

1. Why Bill 64 matters beyond Québec

Two main factors make Bill 64 relevant beyond Québec's borders. First, Québec takes the view that its privacy legislation applies to all collection of personal information in Québec, irrespective of the organization's general regulatory framework. Consequently, Québec's privacy regulator, the Commission d'accès à l'information (CAI), has regularly exercised its jurisdiction over organizations recognized as federal works, undertakings or businesses, entities that are governed by the *Personal Information Protection and Electronic Documents Act* (PIPEDA). This stance significantly broadens the relevance of Bill 64.

Second, as stated above, Bill 64 sets a precedent in Canadian privacy law. Inspired by the *General Data Protection Regulation* (GDPR), Bill 64 raises the bar by introducing new standards for individual privacy rights, establishing standards that are already gaining traction beyond the province's borders. When reading the Government of Ontario's white paper regarding the province's intentions for its own private sector law as well as Ontario's Information and Privacy Commissioner's response to it, one is struck by the number of references to Bill 64 in support of similar enhanced protections for individuals in Ontario.

So the question is, how to best prepare for these substantive changes to Canada's privacy regulatory framework?

2. How to prepare for “post-Bill 64”

Some of the changes proposed in Bill 64 have been common practice for many years, despite not being mandated in Québec. These should not present complex implementation challenges for organizations. For example, organizations will now be required to designate an individual responsible for compliance with privacy legislation. This obligation already exists in various other regimes such as in PIPEDA, and the practice is implemented in most organizations as

best practice. Similarly, Bill 64 introduces mandatory breach reporting, which already exists under other Canadian privacy laws such as Alberta's *Personal information Protection Act* and PIPEDA. Organizations are generally in a position to comply with such obligations. Other provisions of Bill 64, however, introduce new privacy rights and obligations, requiring new corporate processes, policies and technology.

- **Mandatory Privacy Impact Assessments (PIA)**

Québec law will now require PIAs with respect to: i) any project of acquisition, development and redesign of an information system project or electronic service delivery project involving personal information, ii) the transfer of personal information outside of Québec and iii) the communication of personal information without consent for study, research or statistics.

This new requirement entails both governance and policy changes, and the practice must be supported by internal guidelines for staff.

To prepare:

With respect to data governance, organizations should establish a process to facilitate the communication and cooperation between staff and the person in charge of the protection of personal information, regarding any project or initiative that may correspond to one of the situations requiring a PIA.

With respect to policy, organizations should develop a method to perform the required PIAs that best corresponds to their operations. Considering that PIAs have been mandated for certain initiatives of the federal government for decades, it would be wise for organizations to review the Treasury Board of Canada's Directive on Privacy Impact Assessment, as a starting point, to build and implement a similar policy instrument.

With respect to guidelines, staff will need them when making decisions regarding the processing, including storage of personal information outside Québec. Organizations are now required to assess the "*legal framework applicable in the State in which the information would be communicated, including the data protection principles in the foreign state*" and consider sensitivity of the information in order to communicate personal information outside of Québec. The assessment must establish that the information would receive an "adequate" protection in the foreign jurisdiction. Such determinations are complex and staff completing these assessments and negotiating with service providers will need clear guidance in order to comply. Corporate guidelines could spell out a review process and specific criteria, and perhaps even identify countries that offer protections that the organization deems acceptable for the lawful transfer of personal information.

- **Enhanced consent and transparency obligations**

Bill 64 refines existing transparency requirements and introduces new ones to support valid consent from individuals. Consent must be specific to each use of personal information and implied consent is only accepted where some conditions are met. For example, implied consent may not be relied upon for the processing of sensitive personal information, as "opt-in" or express consent is required. As part of the amendments, "*medical, biometric or otherwise intimate information*" is now specifically considered as sensitive by nature, while the contextual analysis to determine whether any other type of information is sensitive in the circumstances, remains.

To prepare:

Organizations should revisit their consent mechanisms and privacy policies to ensure these comply with the amendments, such as obtaining specific consent for each purpose. Organizations should also review their publicly accessible privacy policies to ensure they make the required disclosures to individuals, for example by including detailed information in clear and simple language regarding the organization's use of automated decision-making.

- **Regulation for de-identified and anonymized information**

Bill 64 regulates the use of de-identified and anonymized information. In the Bill, “de-identified information” means information that “*no longer allows the person concerned to be directly identified*”, the operative term being “directly”. Anonymized information, according to the Bill, means that “*it is at all times reasonable to expect in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly*”, the operative terms being “irreversibly” and “directly or indirectly”. The distinction is critical as it determines the permitted use for either type of information. For example, an exception to consent for the use of *de-identified* information is included in the Bill, as long as the use is necessary for study or research purposes, or for the production of statistics. De-identified information is still personal information, and therefore subject to restrictions and requirements, such as the positive obligation for organizations using de-identified information to take reasonable steps to reduce the risk of anyone identifying a natural person using de-identified information.

Once the organization achieves the purposes for which the personal information was collected, the Bill proposes two options: first, it can destroy it, or alternatively, it may anonymize it “*for a serious and legitimate purpose*” according to “*generally accepted best practices*.”

To prepare:

The new definitions clarifying the meaning of “de-identified” and “anonymized” information require that organizations engaging in anonymization practices take a careful look at their technological processes in order to ensure each standard is met and that the organization’s use of each type of information is compliant.

Organizations should also take note that the Bill subjects to high monetary penalties the unlawful re-identification of a person by using de-identified information without authorization or by using anonymized information, as well as any attempt to do so. The maximum fine attached to the penal provisions in the Bill is CA\$100,000 for an individual and CA\$25 million or 4% of the previous year’s global revenue for a corporation. Considering these important fines, organizations should ensure they have robust internal compliance measures in that regard.

- **Regulated automated decision-making**

Taking its cue from the GDPR, Bill 64 introduces requirements related to the use of automated decision-making involving personal information. The terms refer particularly to decisions based exclusively on automated processes, which are understood to refer to decision made without the intervention of a human being.

To prepare:

To meet the requirements of Bill 64, organizations using automatic decision-making will need to update their privacy policies and create new individual rights mechanisms. Specifically, their privacy policies must disclose to individuals the use of automated decision-making processes, no later than at the time it informs the individual of the decision. They will also have to establish a process for individuals to request access to the personal information used to render the decision, the reasons and the principal factors and parameters that led to it, and the information used to make the decision corrected, as applicable. Organizations will also have to establish a process to give individuals the “*opportunity to submit observations*” regarding the decision.

- **A new right to data portability**

The United States has already legislated on the right to portability in certain areas, bringing to light the significant technological challenges and complexities of developing the interoperable infrastructure required to give effect to it. Bill 64 affords organizations a transition period of three years after the date of assent to develop and install the

mechanisms necessary to transfer personal information “*in a structured, commonly used technological format*”. Experience shows that it is an onerous and complex task, which requires time and resources.

To prepare:

In addition to developing the technological infrastructure needed to fulfill portability requests, organizations will need to develop guidelines for their staff to adequately respond to such requests. As the right only applies to “*computerized personal information collected from the applicant, and not created or derived from personal information about the applicant*”, staff will require guidance and training on distinguishing the personal information to be communicated, and the ways of communicating it.

● Enforcement

Moving away from an Ombudsman model where the regulator makes recommendations to organizations, Bill 64 allows the CAI to impose heavy monetary administrative penalties for violations of the Act. These penalties may reach CA\$50,000 for individuals and the greater of CA\$10 million or 2% of the global turnover from the previous year for organizations. Where a violation constitutes an offence under the Act, fines may be imposed of up to CA\$100,000 for an individual and \$25 million or 4% for an organization global turnover of the previous year.

To prepare:

The new financial risk of privacy violations calls for commensurate strengthening of internal compliance processes. Organizations should clarify their data governance structure to ensure clear accountabilities and update their privacy program to assign obligations. If they have not already done so, organizations should adopt robust administrative safeguards such as breach management procedures and protocols to react to a security incident in compliance with the Act.

These organizational measures will both support compliance to avoid penalties and demonstrate due diligence.

● Introducing the “*right to be forgotten*”

Bill 64 also borrows from the GDPR the notion of the “right to be forgotten”. On the model of the GDPR, individuals may require organizations to cease disseminating personal information or to “de-index” a hyperlink attached to their name, that provides access to information by technological means, provided that certain conditions are met.

In addition to the “right to be forgotten”, the individual has the right to require that an organization rectify information if the information is “inaccurate, incomplete or equivocal” or if collecting, communicating or keeping it are not authorized by law. If this information is obsolete or not justified by the purpose of the file, the individual may request that this information be deleted.

To prepare:

Implementation of the right to be forgotten will require delicate balancing between the right of the consumer to have information taken down and the impact of removing information from circulating freely on the internet.

Bill 64 provides a list of factors to take into account when assessing these requests, but organizations must develop guidelines to address the competing considerations they engage. The establishment of such guidelines will be a critical component of each organization’s governance structure to ensure proper implementation to avoid complaints.

3. What to do now?

Make a plan. Organizations should assign to an individual, internal or external to the organization, the task of identifying the changes required in the organization to ensure compliance with Bill 64, the resources required, and the process to follow. Bill 64`s transition periods of one, two and three years will go by quickly.

If you have any questions, please feel free to reach out to Chantal Bernier, Alexandra Quigley or Sasha Coutu with any inquiries.

Your Key Contacts



Chantal Bernier

Of Counsel, Ottawa

D +1 613 783 9684

chantal.bernier@dentons.com



Alexandra Quigley

Senior Associate, Montréal

D +1 514 878 5856

Alexandra.quigley@dentons.com



Sasha Coutu

Associate, Ottawa

D +1 613 288 2708

sasha.coutu@dentons.com