

Bill 64

Québec's Bill 64 proposes to modernize privacy laws



Bill 64, the proposed legislation also known as the *Act to Modernize Legislative Provisions as Regards the Protection of Personal Information*, seeks to **overhaul the framework** applicable to the protection of personal information in various Acts in Québec, including the *Act respecting Access to documents held by public bodies*, and the *Act respecting the protection of personal information in the private sector*. The bill attempts to **modernize the standards** of protection of personal information and grants individuals further control and transparency over the processing of their personal information.

SCOPE

We focus here on the significant changes Bill 64 brings to our organizations, mainly through the modernization of the *Act respecting the protection of personal information in the private sector*. The latter applies to any enterprise, in line with the definitions used by the Civil Code of Québec, that collects, holds, uses or communicates personal information. This can include functions such as the following.



Identification



Tracking



Profiling of the person concerned



Use of personal information

DATA BREACHES INVOLVING PERSONAL INFORMATION

- ◆ If a data breach involving personal information presents a risk of serious harm, the enterprise must promptly notify the **Commission d'accès à l'information (CAI)** and any person whose personal information is affected.
- ◆ Enterprises will be required to keep a record of confidentiality incidents involving **personal information**.
- ◆ Organizations may also notify any third party that could reduce the risk, by communicating only the personal information necessary for that purpose without the consent of the person concerned. In the latter case, the person in charge of the protection of personal information must record the communication of the information.

TRANSPARENCY

The bill requires public bodies and enterprises to publish rules governing personal information and, for those who collect personal information by technological means, to publish and disseminate a **confidentiality policy**.

BROADER ORDER-MAKING POWERS

The bill makes amendments to the functions and **powers of the CAI**.¹

The bill gives the CAI the power to impose penalties of up to

\$10m

OR

2% of worldwide turnover for private sector enterprises.

The bill also gives the CAI the power to initiate criminal proceedings before the courts in the event of a violation of the law.

Enterprises violating the provisions of the bill could be fined between

\$15k

\$25m

OR

4% of worldwide turnover.

CHIEF PRIVACY OFFICER

The bill requires the appointment of a Chief Privacy Officer to be responsible for **protecting personal information**, and therefore for ensuring that this proposed legislation is complied with and enforced.

¹ Commission d'accès à l'information du Québec

THIRD PARTY MANAGEMENT

An enterprise may, without the consent of the person concerned, communicate personal information to any person or body if the information is necessary for carrying out a mandate or performing a contract of enterprise or for services entrusted to that person or body. Enterprises using such subcontractors to process personal information must:

- ✓ Confirm the engagement or contract in writing.
- ✓ Indicate in the engagement or contract the measures to be taken by the agent or person executing the contract to ensure protection of the confidentiality of the identifiable personal information disclosed.

PRIVACY IMPACT ASSESSMENT

The Québec bill requires public bodies and enterprises to conduct a privacy impact assessment **of any information system or electronic service delivery project involving:**



SECURITY

- ▶ Organizations must 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.
- ▶ Bill 64 also requires organizations to ensure that the configurations, user settings and other technological aspects relevant to their offerings are set to the highest levels of confidentiality by default.

CONSENT / PURPOSES FOR USE OF PERSONAL INFORMATION

The bill sets out various consent requirements for the collection, use or disclosure of personal information.

Personal information may be used within the enterprise only for the purposes for which it was collected, unless the individual concerned consents. This consent must be explicit in the case of sensitive personal information. The bill also requires the consent of the holder of parental authority for the collection, use or disclosure of personal information concerning a minor under 14 years of age.

Personal information may, however, be used for other purposes without the consent of the person concerned **only in the following cases:**

- 1** Where it is used for **purposes consistent** with those for which it was collected.*
- 2** Where its use is **clearly for the benefit** of the person concerned.
- 3** Where it is used for **study, research or statistical purposes** and the information is de-identified.

Relevant and direct link to the purpose for which the information was collected. However, **commercial or philanthropic prospecting is not considered a compatible purpose.*



RIGHTS OF INDIVIDUALS

The bill establishes the right of individuals to access or have disclosed to a third party computerized personal information about them in a **structured and commonly used technological format, and the right to have such personal information corrected.**

The bill grants rights to individuals affected by personal information, including the right to require that such information cease to be disseminated **or that any hyperlink attached to their name that provides access to the information by a technological means be de-indexed or re-indexed.**

The bill provides for the right to erase. That is, individuals whose information held by an enterprise can have it deleted when its collection is not authorized by law or when the purpose for which it was collected is achieved.

TRANSFERS OUTSIDE QUÉBEC

The bill provides that before disclosing personal information outside Québec, a person carrying on an enterprise must **conduct a privacy impact assessment**.



The disclosure may be made if the assessment shows that the information would benefit from protection equivalent to that provided for by the bill.

The **privacy impact assessment** must in particular address the following elements:

- ✓ The sensitivity of the information
- ✓ The purpose of its use
- ✓ The protection measures that would apply
- ✓ The legal framework applicable in the state where the information would be disclosed, including its degree of equivalence with the personal information protection principles applicable in Québec



The disclosure must be the subject of a written agreement taking into account the results of the assessment and, if applicable, the terms and conditions agreed to mitigate the risks identified by such assessment.



The same applies when an enterprise entrusts a person or organization outside Québec with the task of collecting, using, disclosing or retaining personal information on its behalf.

How EY can help

At EY, we believe that a strong business reputation needs a robust data privacy program. In addition, organizations need to develop processes and capabilities to embed data privacy in day-to-day activities and support compliance efforts across all areas of operations.

Our services are rooted in the experience we've gained from assisting organizations around the world to help you address your organization's unique and changing requirements in a flexible way.

CATEGORY

KNOWING YOUR CURRENT STATE.

To define an effective and efficient way to respond to privacy considerations, it's imperative to understand what personal information an organization holds, how it is being managed and where it is maintained.

OUR SERVICES

- ▶ Personal information inventory
- ▶ Data mapping
- ▶ Privacy program assessment
- ▶ Privacy impact assessment
- ▶ Artificial intelligence algorithm assessment
- ▶ Third-party (vendor) assessment
- ▶ Cross-border data transfer assessment
- ▶ Internal audit support
- ▶ Privacy program management office
- ▶ Define/review policy framework
- ▶ Design/review processes

DEFINING YOUR FUTURE STATE.

An effective response to privacy regulations requires the definition of a privacy program that enables the continuous demonstration of accountability and compliance. This needs to be enabled through a model that emphasizes accountability, efficiency and effectiveness in the way an organization manages personal information.

- ▶ Privacy program definition and implementation
- ▶ Privacy strategy and roadmap design
- ▶ Digital identity enablement
- ▶ Data privacy breach management and response
- ▶ Data retention and records management program design and implementation
- ▶ Third-party privacy management program design and implementation
- ▶ Privacy awareness, education and training
- ▶ Consent program development
- ▶ Individual's request response procedures design and implementation
- ▶ Cross-border data transfer protection program design and implementation

RESPONDING TO YOUR NEEDS.

Depending on the nature of your business or the challenges your organization are experiencing, you may require very specific and specialized assistance. Our professionals can meet your business requirements with the right privacy context.

- ▶ Privacy managed services
- ▶ Data portability enablement
- ▶ Due diligence privacy assessment for mergers and acquisitions
- ▶ AI governance and ethics program design and implementation
- ▶ Open banking implementation and privacy strategy
- ▶ Trust-by-design implementation



ONE-STOP SHOP FOR ALL YOUR PRIVACY NEEDS

To complement our services, we recently introduced the **EY Data Protection and Privacy Manager**, a customizable, one-stop cloud-based platform that helps organizations track and prioritize their shifting privacy compliance needs. As a managed solution, it allows for unified access to global EY Law, Consulting and forensic capabilities.



CONTACT US

For more information, please contact one of our professionals.



Yogen Appalraju
Partner and Canadian Cybersecurity Leader
Toronto, Ontario
yogen.appalraju@ca.ey.com
+1 416 943 5902



Nicola Vizioli
Partner, Cybersecurity
Montréal, Québec
nicola.vizioli@ca.ey.com
+1 514 879 8046

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2021 Ernst & Young LLP. All Rights Reserved.
A member firm of Ernst & Young Global Limited.

3697960
ED 00

This publication contains information in summary form, current as of the date of publication, and is intended for general guidance only. It should not be regarded as comprehensive or a substitute for professional advice. Before taking any particular course of action, contact Ernst & Young or another professional advisor to discuss these matters in the context of your particular circumstances. We accept no responsibility for any loss or damage occasioned by your reliance on information contained in this publication.

ey.com/ca