New privacy law in Québec: Impacts for businesses

December 09, 2021

In recent years, the legal framework relating to data protection has evolved rapidly and is becoming increasingly rigorous, not only in Québec but also around the world. With the adoption of Bill 64, an Act to modernize legislative provisions as regards the protection of personal information, significant changes will be introduced to Québec's private-sector data protection framework. It is important that businesses start preparing now for the changes to come.

In their latest webinar, lawyers from the Cybersecurity, Privacy & Data Protection group analyze the consequence of this legislative reform and advise Québec businesses on how they can prepare for compliance. This article summarizes the key impacts for businesses presented in detail in the webinar available here.

New enforcement mechanisms

Presented by Simon Du Perron

Bill 64 introduces three different types of mechanisms to enforce compliance under the *Act respecting the protection of personal information in the private sector* (Private Sector Act), namely administrative monetary penalties (AMPs), new penal offences and a private right of action.

The change

Under the new regime, the Commission d'accès à l'information will be able to impose AMPs up to C$10 million or, if greater, two per cent of worldwide turnover. New penal offences are also introduced to the Private Sector with fines of up to C$25 million or four per cent of worldwide turnover. Bill 64 also introduces a new private right of action, which allow individuals to seek punitive damages of at least C$1,000 where an unlawful invasion on privacy causes a prejudice and the infringement is intentional or results from a gross negligence.

How your business can prepare

- Review the Act thoroughly to ensure you are aware of the new grounds for sanctions.

Accountability and Governance

Presented by François Joli-Coeur

Bill 64 applies to anyone operating an "enterprise" within the meaning of the Civil Code of Québec and does not change the scope of the Private Sector Act. It recognizes that each organization is responsible for protecting the personal information it holds. Several new requirements stem from this accountability principle.

The change

By default, the person with the highest authority within the organization (*e.g.* the CEO) will exercise the role of Privacy Officer. This role may however be delegated in writing to a staff member or even to a third party. There is now a formal obligation to establish and implement privacy-related governance policies and practices and to publish detailed information about these on the organization's website. Organizations will be required to conduct privacy impact assessments (PIAs) before the acquisition, development or redesign of an information system or electronic service delivery project involving the processing of personal information. Organizations that collect personal information by offering to the public a technological product or service that has privacy parameters must ensure that, by default, these parameters are set at the highest level of confidentiality.

How your business can prepare

- **Designate a privacy officer**. Establish their **roles and responsibilities** and publish their **contact information** on your organization's website.
- Analyze your business's current policies and procedures, **establish a privacy framework** according to Bill 64's guidelines, and develop a training program for employees to ensure they are aware.
- Develop an **internal PIA procedure**, based on a user-friendly template, and ensure it is adopted widely within the organization.
- Conduct an **inventory of the technological products or services offered to the public** that collect personal information and have privacy parameters.

Transparency and consent

Presented by Éloïse Gratton

Under Bill 64, consent remains the cornerstone of Québec's data protection legal framework. Bill 64 clarifies some rules regarding transparency and consent and introduces new exceptions.

The change

Bill 64 clarifies the transparency and consent rules included in the Private Sector Act. Organizations are required to provide certain information about their data handling practices in “clear and simple language.” Organizations must inform individuals when they collect personal information using a technology that allows the individual to be identified, located or profiled. Organizations that collect personal information through technological means must publish a privacy notice on their website. Bill 64 recognizes that consent may be implied in certain circumstances and it formally requires express consent for the processing of sensitive personal information. Bill 64 also introduces new exceptions for the use and disclosure of personal without consent.

How your business can prepare

- **Review and update privacy notices** for both customers and employees, and update consent forms in plain language.
- **List the different technologies you use to collect personal information** and figure out if any technology is used to identify, locate or profile an individual.
- Update the organization’s **classification policy** to identify information that is sensitive and that belongs to minors.
- **Prepare an inventory of uses and disclosures that may be exempted from the consent requirement** to determine whether they fall within the relevant exceptions.

Research, Analytics and Automated Decision-making

Presented by Max Jarvie

Bill 64 introduces welcome reforms to the regime governing the use and disclosure of personal information in a research context. It also sets out important new requirements in relation to the use of technologies involved in automated decision-making, such as machine learning and other “artificial intelligence” technologies capable of making sophisticated decisions without human supervision.

The change

Bill 64 replaces the current regime regarding the disclosure of personal information for research purposes, which requires the CAI to grant authorization, with a more flexible regime requiring researchers to enter into data sharing agreements and conduct due diligence. Organizations will be able to use personal information, without consent, for purposes that are consistent with those for which the information was originally collected. Bill 64 also introduces another consent exception for the use of personal information for internal study or research if the information is first de-identified. Organizations that use personal information to render a decision based exclusively on an automated processing of such information will have to respect new transparency requirements and give the individual the opportunity to submit observations.

How your business can prepare

- **Implement a procedure for research** projects following the Bill 64 guidelines outlined in this webinar.

- **Be cautious** when using the “consistent purposes” exception for the use of sensitive personal information in internal research. As Max states, “the more sensitive the information, the more likely the regulator is to take a narrow view.”
- **Bear in mind** that the exception for the use of “de-identified data” for research purposes requires organizations to take reasonable steps to reduce the risk of de-identification, and apply stringent measures to avoid re-identification where the personal information underlying the de-identified information is sensitive.
- **Prepare an inventory** of processes that may be subject to the automated decision-making requirements.

New individual rights

Presented by Andy Nagy

The change

Bill 64 grants individuals three new rights in relation to their personal information: the right to control dissemination of personal information (also known as “the right to be forgotten”); the right to data portability; and a right to be informed of, and object to, automated decision making. Bill 64 also reinforces individual control and existing privacy rights by enabling individuals to request further information from organizations about their data processing.

How your business can prepare

- Prepare an inventory of practices that may trigger the application and implement a procedure to reflect these **new individual rights** and implement a procedure **accordingly**.

Outsourcing and Cross-border Transfers

Presented by Elisa Henry

Québec-based organizations that outsource and transfer personal information outside the province face new requirements.

The change

In their privacy notice, organizations must mention the categories of service providers to whom they may transfer personal information. They must also disclose the fact that personal information may be transfered outside Québec. Bill 64 confirms that organizations can share personal information with its service providers without the individual’s consent but both parties must enter into a written agreement containing specific safeguards. Bill 64 provides a new restriction regarding cross-border transfers of personal information, namely a mandatory PIA that must be performed prior to the transfer.

How your business can prepare

- Create a **template data protection agreement** that meets requirements and maps out the service providers.
- Develop an **outsourcing procedure**.
- **Complete a PIA template** to account for risks associated with transfers outside of Québec and conduct a PIA for cross-border processing activities.

Safeguards, Incident response and Biometrics

Presented by Julie Gauthier

The change

Bill 64 introduces a new mandatory private-sector privacy breach reporting regime to the Commission d'accès à l'information. It also provides new requirements regarding the use of biometric systems.

What your business needs to do

- Develop a detailed **incident response plan** based on industry standards;
- **Revise contracts with service providers** to include the new incident reporting obligations;
- Define **a training program** for incident prevention and management;
- **Conduct a privacy impact assessment** prior to any project involving biometric information.
- Establish a directive on the **use of biometric systems**.

BLG's Cybersecurity, Privacy & Data Protection group has recently published a comprehensive Compliance Guide that expands on these changes to help businesses comply with Québec's new privacy requirements.

If you have questions about recent developments regarding the legal framework governing data protection in Québec, reach out to any of the key contacts below.

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.