Québec adopts privacy Bill 64 – Key requirements for businesses

On Sept. 21, 2021, the Québec National Assembly adopted Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, which brings significant changes to Québec private sector and public sector privacy law.

This article focuses on proposed amendments to Québec's *Act respecting the protection of personal information in the private sector* (Private Sector Act) and summarizes the key impact of Bill 64 for businesses in two sections. In Section 1, we present the main new requirements introduced to the Private Sector Act, in order according to the date they come into force. It should be noted that this implementation period begins on September 22, 2021 which is the date of assent of the *Act to modernize legislative provisions as regards the protection of personal information*. In Section 2, we provide a summary of the new enforcement mechanisms for ensuring compliance with the Act.

We invite you to consult our amended version of the Private Sector Act for the exact wording of these amendments.

1 New requirements to the Private Sector Act

The following requirements will come into force in one year

Requirement	Description
Appointment of a Privacy Officer (s. 3.1)	• By default, the CEO of every organization will be the "person in charge of the protection of personal information". • The Privacy Officer must ensure that the organization implements and complies with the Act. • The Privacy Officer role can be delegated in writing to any person. • The Privacy Officer's contact information must be published on the organization's website.
Breach reporting (ss. 3.5 – 3.8)	• Organizations must notify the Commission d'accès à l'information (CAI) and the affected individuals when a "confidentiality incident" presents a "risk of serious injury" to the individuals. • The "risk of serious injury" threshold is assessed using factors similar to the "real risk of significant harm" under PIPEDA, namely the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes. • Organizations must keep a register of breaches that they would be required to provide to the CAI upon request.

The following requirements will come into force in two years

Requirement	Description
Policies and practices (s. 3.2)	• Organizations must establish and implement policies and practices regarding the protection of personal information. • These policies and practices must: – Provide a framework for the keeping and destruction of the information; – Define the roles and responsibilities of the members of its personnel throughout the life cycle of the information; and – Provide a process for dealing with complaints regarding the protection of the information. • Organizations must publish detailed information about these policies and practices on their website.
Privacy impact assessments (PIA) (ss. 3.3 – 3.4)	• Organizations must conduct PIAs with respect to the acquisition, development and redesign of any information system or electronic service delivery project involving the collection, use, communication, keeping or destruction of personal information. • A PIA shall be "proportionate to the sensitivity of the information, the purpose for which it is to be used, and the amount, distribution and format of the information".
Automated processing (s. 12.1)	• Organizations must inform the individual when his or her personal information is used to render a decision based exclusively on an automated processing of such information. • Organizations must also, at the individual's request, inform them about: – the personal information used to render the decision; – the reasons and the principal factors and parameters that led to the decision; and – the right of the individual to have the personal information used to render the decision corrected. • Organizations must also provide the individual with an opportunity to submit observations to a member of the organization who is in a position to review the decision.
Cross-border transfers (s. 17)	• Organizations must conduct a PIA prior to communicating personal information outside of Québec, in order to assess whether the information will receive an "adequate protection" in compliance with "generally accepted data protection principles". • Such PIAs must take into account: – the sensitivity of the information, – the purposes for which it will be used and the protection measures, including contractual ones, that would apply to it; and – the legal framework applicable in the State in which the information would be communicated, including the data protection principles applicable in the foreign State. • This communication will have to be subject to a written agreement that takes into account the results of the PIA and, if applicable, sets out measures to mitigate the risks identified in the PIA.

The following requirements will come into force in **two years**

Requirement	Description
Outsourcing (s. 18.3)	• Organizations that transfer personal information to a service provider must enter into a written agreement with the service provider, which must provide: – A description of the measures taken by the service provider to ensure the confidentiality of the personal information (e.g. a description of the security safeguards); – An obligation for the service provider to only use the information for the purposes of rendering the services and not keep such information after the expiry of the contract; and – An obligation for the service provider to notify the Privacy Officer without delay of any actual or attempted violation of the confidentiality of the information and to allow the privacy officer to conduct any verification relating to confidentiality requirements.
Transparency (s. 8 and 8.2)	• Organizations must provide the following information to individuals upon collection of their personal information: – the purposes of the collection; – the means of collection; – the rights of access and rectification; and – the person's right to withdraw consent to the communication or use of the information collected. • If applicable, the following information must also be provided: – the name of the third party for whom the information is being collected; – the categories of third parties to which it is necessary to communicate the information for the purposes of the collection (i.e. service providers); and – the possibility that personal information could be communicated outside Québec. • Organizations must publish a privacy policy on their website if they collect personal information through technological means. • The privacy policy must be drafted in clear and simple language.
Transparency – Profiling, Geolocation and Identification Technologies (s. 8.1)	• Organizations must inform individuals of any collection of personal information using a technology that includes functions allowing the individual to be identified, located or profiled. • Organizations must also inform individuals of the means available to activate such functions. • "Profiling" refers to 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".

The following requirements will come into force in **two years**

Requirement	Description
Consent (ss. 8.3, 12 and 14)	• Any individual who provides their personal information after receiving an adequate privacy notice is deemed to have consented to its use and its communication for the purposes indicated in the notice. • Consent must be clear, free and informed and be given for specific purposes and must be requested for each such purpose, in clear and simple language and separately from any other information provided to the individual. • Organizations must obtain express consent to use sensitive personal information for secondary purposes. • Information is sensitive if, due to its nature, including medical, biometric or otherwise intimate information, or the context of its use or communication, it entails a high level of reasonable expectation of privacy. • Consent of a minor under 14 years of age must be given by the person having parental authority or by the tutor. • Organizations will benefit from new consent exceptions.
Privacy by default (s. 9.1)	• Organizations that collect personal information by offering to the public a technological product or service that has privacy settings must ensure that those settings provide the highest level of confidentiality by default. • This requirement does not apply to cookies.
Retention and destruction (s. 23)	• Once the purposes for which personal information was collected or used are achieved, organizations must destroy the information. • They may also anonymize the information, according to generally accepted best practices, in order to use it for a serious and legitimate purpose.
De-indexation right (s. 28.1)	• Individuals may request that organizations cease disseminating their personal information and de-index any hyperlink attached to their name that provides access to the information if the dissemination contravenes the law or a court order.

The following requirements will come into force in **three years**

Requirement	Description
Data portability right (s. 27)	• An individual may request that personal information collected from them be communicated to them (or to another organization designated by the individual) in a structured, commonly used technological format. • This excludes personal information that the organization has created or inferred from the individual's personal information. • The organization is not required to destroy the personal information after processing a portability request.

2 Enforcement

The Private Sector Act will now have three unique compliance mechanisms:

1. Administrative monetary penalties (AMPs) enforced by the Commission d'accès à l'information (CAI)
2. New penal offences with hefty fines.
3. A private right of action allowing individuals to sue an organization for damages.

The following table provides a summary of the key offences that may be subject to sanction under this new enforcement regime which will come into force in two years.

Violation	Penal Offences	AMP	Private Right of Action
Collection, use, disclosure or destruction of personal information in contravention of the Act →	X	X	X
Retention of personal information in contravention of the Act →		X	X
Failure to provide an appropriate privacy notice →		X	X
Failure to notify the CAI or the affected individuals of a breach that presents a risk of serious injury →	X	X	X
Failure to inform the individual concerned by an automated decision or to provide an opportunity to submit his observations →		X	X
Refusing or failing to comply with a request for production of documents issued by the CAI within the specified timeframe →	X		
Failure to comply with an order issued by the CAI →	X		
Penalty (Maximum Amount)	**$25 million or 4 per cent of worldwide turnover**	**$10 million or 2 per cent of worldwide turnover**	**Damages awarded**

Next steps

BLG will soon publish a comprehensive guide to help businesses comply with the new privacy requirements introduced by Bill 64.

For any questions you may have about recent developments regarding the legal framework governing data protection in Québec, please reach out to a key contact below or a member of BLG's Cybersecurity, Privacy & Data Protection team.

Katherine Poirier
Partner
T 514.954.3175
kpoirier@blg.com

Frédéric Wilson
Counsel
T 514.954.2509
fwilson@blg.com

Patrick Laverty-Lavoie
Senior Associate
T 514.395.3887
plavertylavoie@blg.com

Candice Hévin
Senior Associate
T 514.954.2588
chevin@blg.com

Simon Du Perron
Associate
T 514.954.2542
sduperron@blg.com

Borden Ladner Gervais