June 15, 2020

ARTICLE

Proposed amendments to Québec privacy law: Impact for businesses

On June 12, 2020, the day before the Québec National Assembly adjourned until September 2020, the Government of Québec introduced Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*. The proposal would bring 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*.

This article summarizes the key impact of Bill 64 for businesses.

What you need to know

Major changes to the current legislative framework include:

- New enforcement tools:
  - The Commission d'accès à l'information (CAI) would have powers to impose administrative monetary penalties of up to C$10,000,000 or, if greater, the amount corresponding to 2 per cent of worldwide turnover in the preceding year.
  - Reinforced fines in the case of penal proceedings of a maximum of C$25,000,000, or, if greater, the amount corresponding to 4 per cent of worldwide turnover for the preceding fiscal year.
  - New private right of action for individuals.
- New breach reporting requirements.
- New requirements for outsourcing and transfers outside of Québec, including an adequacy system seemingly influenced by European law.
- New individual rights inspired by European law: right to data portability, right to be forgotten and right to object to automatic processing.
- New accountability rules:
  - Introduction of a new privacy officer role that would rest with CEOs by default.
  - New obligation to establish, implement and publish governance policies and practices.
  - New obligation to conduct privacy impact assessments (PIAs).
  - Privacy by design requirements.
- Reinforced consent requirements (including explicit requirements to obtain express consent in certain situations).
- New transparency requirements, including when organizations are using technologies allowing individuals to be identified, located and profiled.
- Some less stringent rules:
  - New consent exceptions for research and business transactions.
  - Exclusion of business contact information from the definition of "personal information."

Introduction

- Québec's *Act respecting the protection of personal information in the private sector* (Private Sector Act), which was adopted in 1993, was the first private-sector privacy law in Canada. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), the Alberta *Personal Information Protection Act* (Alberta PIPA) and the British Columbia *Personal Information Protection Act* (BC PIPA) came about 10 years later.With Bill 64, Québec might become the first Canadian jurisdiction to follow the new trend of stronger privacy laws initiated by European Union's General Data Protection Regulation (GDPR) and more recently, the *California Consumer Privacy Act of 2018* (CCPA).

Enforcement

Bill 64 would make the CAI the first Canadian privacy regulator with powers to directly impose administrative monetary penalties (AMPs) to organizations for privacy violations. It would also reinforce the current penal regime and introduce a new private right of action.

Administrative monetary penalties

The AMPs would apply to a broad range of contraventions: failure to comply with transparency requirements; collection, communication, use or destruction of personal information in contravention of the statute; failure to report a breach; and non-compliance with the automated decisions provision (s. 90.1). For businesses, the CAI would be empowered to impose penalties of a maximum of C$10,000,000 or, if greater, the amount corresponding to 2 per cent of worldwide turnover for the preceding fiscal year (s. 90.12). Bill 64 would require that the CAI develop and make public a general framework for the application of AMPs, specifying various elements listed in the bill (s. 90.2). Bill 64 provides for a notification procedure before the imposition of an AMP (s. 90.3 and 90.4), an internal review process (s. 90.6, 90.7 and 90.8) and a right to contest the review decision before the Court of Québec.

Penal regime

The Private Sector Act currently includes a penal regime allowing the province's attorney general to seek fines before the courts for violation of the statute. However, these provisions have never been used. Under Bill 64, the CAI would be empowered to institute penal proceedings. Bill 64 would also substantially increase the potential fines. From the current maximum of C$10,000 for a first offence and C$20,000 for a second, the maximum fine would become C$25,000,000, or, if greater, the amount corresponding to 4 per cent of worldwide turnover for the preceding fiscal year (s. 91). In the case of a subsequent offence, the fines would be doubled (s. 92.1). The penal regime applies to more offences than the AMPs, including: interfering with the CAI's investigation and identifying or attempting to identify a natural person by using de-identified information without the authorization of the person holding the information or by using anonymized information (s. 91).

Private right of action

Individuals are currently able to bring privacy actions before Québec courts for privacy violations based on the privacy provisions of the Civil Code of Québec. Bill 64 would create a private right of action allowing individuals to be compensated for the unlawful infringement of a right conferred by the statute or the privacy articles of the Civil Code, unless the damage results from "superior force" (s. 93.1). This provision may translate in Québec becoming an even friendlier jurisdiction for privacy class actions. The statute also provides for the award of punitive damages of at least C$1,000 where the infringement is intentional or results from a gross fault.

Accountability

Unlike PIPEDA, the Private Sector Act does not put a strong and explicit emphasis on accountability. This would change as Bill 64 introduces a new privacy officer role, an obligation to implement and publish policies and practices relating to the protection of personal information, an obligation to conduct privacy impact assessments (PIAs) and privacy by design requirements.

Introduction of a privacy officer role for the CEO

The *Private Sector Act* does not explicitly require that organizations designate a person accountable for the organization's compliance with the statute, as opposed to PIPEDA. Bill 64 would create a new privacy accountability role within the organization that resembles the data protection officer (DPO) role under the EU General Data Protection Regulation. By default, the CEO would be the "person in charge of the protection of personal information" (for convenience, we refer to this role as the "privacy officer" in this article) and would bear the responsibility of ensuring that the enterprise implements and complies with the Act (s. 3.1). That person would be able to delegate all or part of that function in writing to a personnel member. This person's contact information would have to be published on the enterprise's website (or by another appropriate method if the enterprise does not have a website).

Policies and practices

Bill 64 introduces another significant requirement related to accountability: enterprises in Québec would have to establish and implement governance policies and practices regarding the protection of personal information. These policies 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" (s. 3.2). Surprisingly, enterprises must publish these policies and practices on their website. We expect the industry to ask for clarification regarding this provision as it seems to require the publication of internal policies. Unlike privacy policies or notices that organizations typically publish on their website pursuant to the transparency requirement (specifically addressed at section 8 of the bill), organizations generally do not publish their internal privacy policies and procedures.

Mandatory privacy impact assessments

Bill 64 requires enterprises to conduct an "assessment of the privacy-related factors" with respect to any "information system project" or "electronic service delivery project" involving the processing of personal information (s. 3.3). This activity is commonly known as a "privacy impact assessment" (PIA). A PIA is a process that enables an organization to review an initiative, program or project involving the collection, use or disclosure of personal information in order to identify applicable legal requirements, assess potential privacy risks and mitigate those risks to an acceptable level through a combination of measures.

While the Private Sector Act does not currently refer to the concept of PIAs, it is considered a best practice under Canadian private-sector privacy laws (and is often mandatory in the public sector). Bill 64 would significantly expand the number of instances in which an organization would have to conduct PIAs, as it would likely extend to most e-commerce activities and data processing systems.

Privacy by design

Bill 64 would require enterprises collecting personal information through technological goods or services to follow a "privacy by design" approach. In particular, organizations would have to ensure that the parameters of their technological products or services provide the "highest level of confidentiality by default, without any intervention by the person concerned" (s. 9.1).

A privacy by design approach seeks to ensure that individuals' privacy rights are respected at every stage of an initiative's development and renders all stakeholders accountable for making a particular product or service privacy-protective by default. This approach is expressly found under Article 25 of the GDPR, and was endorsed in a recent Report of the Standing Committee on Access to Information, Privacy and Ethics concerning the review of PIPEDA. Yet, unlike the GDPR, which expressly takes into account the circumstances surrounding a particular initiative, including the costs of implementation and degree of risk for individuals involved, the proposed section 9.1 does not provide any qualifier with respect to what will be considered the "highest level of confidentiality" in a given context. Future amendments or guidance might clarify the scope of this provision in a manner that takes into account reasonable commercial considerations and business models.

New breach notification requirements

With British Columbia, Québec is the only jurisdiction in North America that does not mandate breach reporting. This would change with Bill 64, which introduces breach notification requirements similar to PIPEDA and the Alberta PIPA (s. 3.5). The requirement to notify the CAI and the affected individuals is triggered 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 (s. 3.7). Similar to PIPEDA, enterprises would have to keep a register of breaches that they would be required to provide to the CAI upon request (s. 3.8).

Bill 64's breach notification requirements cover incidents involving the unauthorized use of personal information, whereas the common approach for breach notification requirements in Canada and globally (including under the GDPR and U.S. state breach notification laws) is to focus on unauthorized access to, disclosure or loss of personal information. It will be important to follow the developments of Bill 64, because as currently drafted, organizations operating in Québec may have to comply with enhanced notification requirements.

Transparency and consent

In principle, the Private Sector Act requires obtaining manifest, free and enlightened consent, which must be given for specific purposes in order to collect, use or communicate personal information. Bill 64 provides more details around the type of information that must be available to individuals upon collecting their information, new requirements to obtain express consent in certain situations, new restrictions when dealing with children under 14 years of age, new consent exceptions covering business contact information and the sharing of personal information in the context of commercial transactions. It also introduces an obligation to inform individuals of the use of a technology that allows them to be identified, located or profiled.

Transparency and privacy policy

Bill 64 introduces a new section under which certain specific information must be made available upon the collection of personal information (s. 8). This includes 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 individual must be informed of the name of the third person for whom the information is being collected and of the possibility that the information could be communicated outside Québec. On request, the person concerned must also be informed of the personal information collected from him, the categories of persons who have access to the information within the enterprise, the duration of the period of time the information will be kept and the contact information of the person in charge of the protection of personal information. This information must be provided to the person concerned in clear and simple language, regardless of the means used to collect personal information.

Reinforced consent

The Private Sector Act does not currently expressly refer to the concepts of express and implied consent (consent must be "manifest, free, and enlightened, and must be given for specific purposes").Meanwhile PIPEDA, the Alberta PIPA and the BC PIPA authorize implied consent under certain circumstances. Bill 64 provides that personal information may not be used, except for the purposes for which it was collected or communicated to a third person unless the person concerned gives their consent or the law provides for the communication (s. 12 and 13). Such consent must be given expressly when it concerns sensitive personal information (s. 12 and 13), which implies that another form of consent may be acceptable in some situations involving non-sensitive information. Personal 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. In any event, 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 person concerned (s.14). We expect the industry to ask for clarification regarding this provision as it is unclear if "separately from any other information provided to the person concerned" means outside the scope of a privacy policy.

Secondary uses and enterprise analytics

There is some flexibility introduced for secondary uses of personal information. Bill 64 provides personal information may be used for another purpose without the consent of the person concerned if it is used for purposes consistent with those for which it was collected (*i.e.* it must have a direct and relevant connection with such purposes which must be other than commercial or philanthropic prospection), or clearly used for the benefit of the person concerned. Furthermore, there is some flexibility introduced for research, study or research or for the production of statistics, which is discussed further under section "Consent exception for de-identified personal information".

Dealing with children

Bill 64 introduces a new section under which the personal information concerning a minor under 14 years of age may not be collected without the consent of the person having parental authority, unless such collection is clearly for the minor's benefit (s. 4.1). The consent of a minor under 14 years of age must be given by the person having parental authority and the consent of a minor 14 years of age or over can be given either by the minor or by the person having parental authority (s.14).

Business transaction exception

When a business is being purchased or sold or when assets are being acquired or assigned, it may in practice be fastidious—even impossible—to obtain consent to the disclosure of personal information by all customers, employees and other parties contemplated by the transaction, whether at the stage of due diligence verification or at the closing of a transaction. To respond to this problem, PIPEDA, PIPA (BC) and PIPA (Alberta) include exceptions to consent that are specific to business transactions. Bill 64 now also introduces such exception for business transaction, which is aligned with these laws. Under such new exception, only the personal information necessary for concluding the commercial transaction may be communicated to the other party without the consent of the person concerned and these parties must comply with certain requirements:

- Entering into an agreement containing certain specific limitations and security provisions;
- Upon the commercial transaction concluded, the acquirer may only use or communicate the personal information in compliance with the Private Sector Act; and
- Within a reasonable time after the conclusion of the commercial transaction, persons concerned must be notified of the transaction (s. 18.4).

Business contact exclusion

Bill 64 modifies the Private Sector Act by including a full exclusion for business 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" (s. 1). This exclusion is aligned with the BC PIPA but goes beyond the business contact exclusion under PIPEDA and the Alberta PIPA which is limited to a situation where the purposes of collecting this information is restricted to enabling the individual to be contacted in relation to the individual's business responsibilities.

No employee consent exception

Bill 64 does not include an employee consent exception. This is problematic since the consent model appears ill-suited to an employer/employee relationship. Indeed, it is difficult to think of an employee's consent in dealing with their employer as being "free," since an employee could well believe, rightly or wrongly, that their employment would be jeopardized by a refusal to consent. Moreover, if an employee refused their employer's collecting, using or disclosing of their personal information for normal employment purposes, this could simply prevent the employer from continuing its activities and fulfilling its legal obligations. Under PIPEDA, BC PIPA and Alberta PIPA, employers may collect, use and disclose personal information that is necessary for establishing, managing or terminating an employment relationship without the consent of their employees, although they have a duty to inform employees of their practices. Hopefully such exception will be introduced and considered by the legislator in the next stages.

Obligation to inform individuals of the use of a technology that allows them to be identified, located or profiled

Bill 64 would require that, before collecting personal information using technology which allows an individual to be identified, located or profiled, an organization inform the individual of the use of such technology and the means available, if any, to deactivate the functions that allow them to be identified, located or profiled (s. 8.1). The notion of "profiling" is broadly defined under the new section as the collection and use of personal information to assess particular characteristics of a natural person, including their work performance, health, preferences, behaviour, interests, etc.

The proposed provision does not strictly require an organization to provide individuals with an opt-out mechanism with respect to its use of identification, tracking or profiling technologies. That said, in certain cases, express consent may also be required as discussed under Reinforced consent. In addition, more transparency may become expected from organizations using a variety of third-party analytic tools and software, including cookies, pixels and beacons, to track, identify and target individuals based on their interests, preferences and behaviour. These tools often come with an opt-out mechanism accessible through the service provider's platform and organizations would be required to communicate them to users.

Research and analytics

Bill 64 introduces welcome reforms to the regime governing the use of personal information in the context of research, aligning Québec with the frameworks established in other Canadian jurisdictions. It also introduces important flexibility with respect to secondary research purposes, such as enterprise analytics, by clearly permitting the use of "de-identified" personal information (including sensitive information) within the enterprise without obtaining consent.

Consent exception for research

Bill 64 eliminates the authorization process for research, long criticized for its impractical complexity and for the uncertainty created by the CAI's total discretion over research authorizations and the revocation thereof. Amendments replace the current process with a regime that emphasizes due diligence and transparency, and only requires that the CAI be notified of the agreement entered into between the disclosing and recipient organizations. Under the new framework, an organization may disclose personal information, without the consent of the individual concerned to a person or body wishing to use the information for study or research purposes or for the production of statistics, provided that:

- The objective of the research can be achieved only if the information is communicated in a form allowing the persons concerned to be identified;
- It is unreasonable to require the person or body to obtain the consent of the persons concerned;
- The objective of the research outweighs the impact of communicating and using the information on the privacy of the persons concerned;
- The personal information is used in such a manner as to ensure confidentiality; and
- Only the necessary information is communicated (s. 21).

Requests must be in writing and include the research protocol, the grounds supporting the fulfilment of the abovementioned criteria, a list of the other persons and bodies whose information is being requested, a description of the technologies being used if applicable and a copy of the documented decision of a research ethics committee if applicable (s. 21.01). The person disclosing and the recipient must enter into an agreement that includes a variety of stipulations intended to ensure limited access, reduced risk of re-identification, appropriate security safeguards and minimal retention (s. 21.02). The agreement must be sent to the CAI such that it comes into force 30 days following receipt. In this latter respect, the new framework aligns with the current PIPEDA regime, which similarly requires the Office of the Privacy Commissioner of Canada (OPC) to be notified.

Consent exception for de-identified personal information

Bill 64 amends section 12 of the Private Sector Act to state that personal information initially collected for one purpose may be used, without consent, for the secondary purposes of study or research or for the production of statistics, if the information is de-identified (s. 12, paragraph 2(3)). The amended section also states that personal information is "de-identified if it no longer allows the person concerned to be directly identified" (s. 12, paragraph 4(1)). This aligns with the core features of the notion of pseudonymized information, as this term is generally understood (including under the GDPR): the removal of all "direct identifiers" (e.g. name, social insurance number), while leaving "indirect identifiers" (date of birth, gender) intact. Underscoring this understanding of de-identification, Bill 64 also introduces criteria for anonymization, stating "[f]or the purposes of this Act, information concerning a natural person is anonymized if it irreversibly no longer allows the person to be identified directly or indirectly" (s. 23, emphasis added). In consequence, it appears that the amended section 12 implicitly recognizes the risk of re-identification attached to de-identified information. Interestingly, the language of the new section 12 also clearly provides that no consent is needed even where such information is sensitive (s. 12, paragraphs 1-2).

As drafted, this consent exception appears to apply only to use within the enterprise, and as such the purposes of study, research and the production of statistics may be construed as enterprise or business analytics. However, given that identical language is used to describe research under the new section 21 and following, section 12 appears to provide latitude for those enterprises engaged in scientific research to use de-identified personal information without consent for this purpose as well.

New individual rights

Bill 64 grants individuals three new rights with respect to their personal information, inspired by the GDPR. For ease of reference we will refer to as the right to data portability, the right to be forgotten and the right to object to the automated processing of their personal information.

Right to data portability

Bill 64 first clarifies the existing right to access provided at section 27 of the Private Sector Act by granting individuals the right to obtain a written and intelligible transcript of computerized information held about them by an organization. The provision goes further and provides that individuals can request organisations to provide them with computerized personal information in a structured, commonly uses technological format (i.e. an electronic file) and to ask such data "to be communicated to any person or body authorized by law to collect such information". Organizations should take this new right into account at the design stage of their IT projects and online services to ensure that personal information collected from the individual can be communicated to them in the requested format (s.3.3). The only basis upon which organizations can refuse to honour such requests is if "doing so raises serious practical difficulties".

This new provision echoes the right to data portability provided at article 20 of the GDPR, aimed at strengthening individuals' control over their personal information and fostering interoperability between controllers. It will be important to clarify the restriction limiting third party recipients to those "authorized by law to collect such information" and to ensure that the transferred data will not have to be deleted by the transferring organization, who may need it to perform its contractual obligations or to comply with its retention schedule.

Right to be forgotten

The new section 28.1 grants individuals a two-prong right that exists (under a slightly different form) in the European Union since 2014, now codified at article 17 of the GDPR.

The new provision first allows individuals to request organizations to cease disseminating their personal information and to de-index any hyperlink attached to their name that provides access to the information if the dissemination contravenes the law (*e.g.* defamatory content or clear cases of cyber-bullying) or a court order. Website editors and search engines will hence have to not only abide to court orders but also assess whether the impugned content infringes applicable law, raising important questions as to the role played by private organizations in the administration of justice.

Second, individuals are granted a right to request that their personal information ceases to be disseminated or be de-indexed or re-indexed when the dissemination of the information causes serious injury to an individuals' reputation or privacy that clearly outweighs the public's right to be informed and one's freedom of expression (to the extent the sought remedy does not exceed what is necessary for preventing the perpetuation of the injury). Bill 64 provides several criteria to make such assessment, which mirror those commonly taken into account by Canadian courts in privacy and defamation actions. This new right will make it easier for individuals to have harmful content removed from the Internet without having to initiate legal proceedings (including victims of "revenge porn" and unauthorized publications of intimate pictures). These rights also bring many concerns already raised in a prior submission made to the OPC in answer to the consultation relating to online reputation.

Right to object to automated processing

At section 12.1, Bill 64 grants a new right for individuals with respect to the automated processing of their personal information. When an organization uses automated processing of personal information to make a decision about an individual *(e.g.* to offer a product or service based on an assessment of one's financial or medical situation), this provision grants concerned individuals the right to be informed about such processing, including to be provided with information regarding the elements of personal information used, the reasons and principal factors and parameters leading to the decision and the right to have their information corrected. In addition, concerned individuals must be given the opportunity "to submit observations to a member of the personnel of the organization who is in a position to review the decision made by automated means". Automated processing activities that affect individuals must hence, upon request, be reviewed by employees who have the power (and, presumably, the sufficient knowledge) to re-assess computer-made decisions. Interestingly, section 12.1 does not grant individuals a right (such as the one granted in the GDPR at article 22) but rather "an opportunity to present observations", which seem to open the door to organizations' discretion to indeed review or not the automated decision.

Outsourcing and cross-border transfer

Sharing personal information with service providers is subject to requirements set forth at section 18.3 which confirm current best practices. When sharing information with third parties located outside of Québec however, Bill 64 proposes a very burdensome process, which we summarize below.

Outsourcing

Bill 64 formally recognizes that communicating personal information to a service provider (or a mandatary/agent) does not require the consent of the concerned individual (s.18.3), which is a welcomed clarification. Further, in line with the OPC's 2019 Reports of Findings in the Equifax and Loblaw's cases as well as current best contractual practices, the provision requires that outsourcing arrangements be subject to a written agreement entered into by the organization and 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. Regarding this last requirement, Bill 64 does not specify whether the privacy officer is the one of the service provider or of the organization. While we assume that the objective is that the privacy officer of the organization be notified, clarification on this aspect would be welcomed.

Cross-border transfers

A provision of Bill 64 that would create the most challenges for organizations pertains to cross-border transfers. Bill 64 significantly increases the requirements set forth in the current section 17 of the Private Sector Act. Under the proposed text, an organization must, prior to communicating personal information outside of Québec (including for outsourcing purposes), perform a PIA to assess whether the information will receive a level of protection equivalent to the one granted under the Act. To that end, organizations are required to take into account not only the sensitivity of the information, the purposes for which it will be used and the protection measures that would apply but also "the legal framework applicable in the State in which the information would be communicated, including the legal framework's degree of equivalency with the personal information protection principals applicable in Québec". If, following this PIA, the organization concludes that the foreign legislation is not equivalent, it must not communicate the personal information. Section 17.1 of Bill 64 provides that the government shall publish a list of States whose legal framework governing personal information is equivalent to the Québec framework.

It is important to highlight that under the GDPR, a similar exercise is performed by the European Commission after a very detailed and lengthy process involving the European Data Protection Board and the representatives of Member States, to assess whether the legislation of countries outside the European Economic Area is "adequate" in accordance with the Adequacy Referential. This process takes several months and may lead to a finding of inadequacy such as in the case of the Québec proposal in 2014. The fact that European Commission had declared PIPEDA "adequate" in 2001, which is not as stringent as the Private Sector Act in many aspects, further illustrates the challenges with any methodology used to compare laws. If the third country is not considered adequate, different mechanisms can be used by organizations pursuant to the GDPR to transfer personal information outside of the EEA, including standard contractual clauses, binding corporate rules, etc.

Here, the government may have underestimated the efforts that would be required for them to publish a comprehensive list of adequate jurisdictions in accordance with proposed Section 17.1. This may put private organizations in a situation where they need to play the role of a privacy regulator and retain foreign legal experts to assess the equivalency of non-Québec laws. Moreover, Bill 64 fails to provide organizations with alternative mechanisms to transfer information to the rest of the country or abroad. If adopted as currently drafted, this provision will render transfers to service providers located outside of Québec illegal. This appears not only impractical, but also raises important challenges related to data residency.

Next steps

Most of Bill 64's provisions are unlikely to take effect until early 2022. Following the successful introduction of Bill 64 on Friday, June 12, 2020, which is only the first step in Québec's legislative process, the Québec National Assembly adjourned its activities until September 15, 2020. Before adjourning, the government house leader, indicated that the bill would be referred to a committee for consultation, which should give stakeholders the occasion to make representations regarding Bill 64. If passed, Bill 64's transitional and final provisions currently state that the amendments made to Québec's private sector privacy laws would only come into effect one year following the date of the bill's assent, except for the provision on data portability rights, which would only come into effect three years after the date of assent.

The authors gratefully acknowledge the assistance of articling student Andy Nagy in writing this article.

By: Éloïse Gratton, Elisa Henry, François Joli-Coeur, Max Jarvie, Andy Nagy

Services: Cybersecurity, Privacy & Data Protection, Online Retail & E-commerce

Key Contacts

Éloïse Gratton
Partner and National Leader, Privacy and Data Protection

Toronto

EGratton@blg.com

416.367.6225

François Joli-Coeur
Partner

Toronto

FJolicoeur@blg.com

416.367.6178