End of parliamentary proceedings in Quebec: An Update on Bill 64

June 21, 2021

One year after its introduction at the Québec National Assembly, Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (Bill 64) has still not been adopted. With the end of the parliamentary proceedings on June 11, 2021, BLG's Privacy and Data Protection team provides an update on this important reform of Québec's privacy law.

This article will present the key amendments made to Bill 64 during the committee process and their impact on businesses. We invite you to look at our amended version of the *Act respecting the protection of personal information in the private sector* for the specific text of the amendments.[1]

For a detailed analysis of the key issues raised by Bill 64, we encourage you to read our bulletin released at the time of the Bill's introduction in June 2020 or our short submission issued to the Committee in the fall of 2020 in which we provided our observations on the impact that Bill 64 may have on private sector businesses.

We include a recap of the legislative process of Bill 64 in Part I to better contextualise the amendments before diving into this update.

Part 1 – Bill 64's progress since its introduction

Bill 64 introduces significant changes to the two main privacy laws in Québec, namely the *Act respecting Access to documents held by public bodies and the Protection of personal information* (Access to Information Act) and the *Act respecting the protection of personal information in the private sector* (Private Sector Act). Given the scope of this reform, special consultations were held throughout the month of September 2020, during which several stakeholders were given the opportunity to be heard.

The Québec National Assembly's Committee on Institutions subsequently adopted Bill 64, in principle and clause-by-clause consideration, in February 2021. In accordance with the sequence set out in Bill 64, Members of Parliament (MPs) first considered the provisions amending the Access to Information Act before turning to those dealing with the Private Sector Act. That being said, with a few exceptions, given that many of the provisions introducing changes to the public and private sector acts are substantively

identical, the Committee MPs made matching amendments to the public and private sector elements of the Bill as they went.

At the time of adjournment, the Committee was considering section 124 of Bill 64 (out of a total of 165). **It is therefore reasonable to expect Bill 64 to be passed when the parliamentary proceedings resume in the fall of 2021.**

Part 2 – Key changes made in Committee

Before delving into the details of the amendments adopted by the Committee, below is a list of the changes most likely to have an impact on the day-to-day operations of businesses in Québec:

- **Modifications providing more flexibility:**
  - The ability to delegate “the function of the person in charge of the protection of personal information” to any person, whether internal or external to the company.
  - The obligation to conduct a privacy impact assessment is now limited to the “acquisition, development and redesign of an information system” and shall be performed in a manner “proportionate” to information’s sensitivity, purpose of use, distribution amount and format.
  - Personal information may be used without the consent of the person concerned when its use is necessary for the supply or delivery of a product or the provision of a service.
  - Personal information may be used without the consent of the person concerned when its use is necessary for the prevention and detection of fraud or the evaluation and improvement of protection and security measures.
  - The communication of personal information outside Québec no longer requires the State releasing information to apply a legal framework “equivalent” to Québec’s regime. Rather, the information must receive “adequate” protection in compliance with “generally accepted data protection principles”.
- **Modifications imposing more stringent requirements:**
  - Businesses collecting personal information will be required to inform the person concerned of the "name of the third persons" to whom the information may be communicated for the purposes of the collection.
  - When using technologies to collect personal information, functionalities allowing a person to be identified, located or profiled must be deactivated by default; and
  - A business may only anonymize personal information as an alternative to destruction if it is to be used for a “serious and legitimate purpose”.

Accountability

New privacy officer role assigned to the CEO

With respect to the accountability principle, an amendment was adopted to clarify that the function of "person in charge of the protection of personal information", which Bill 64 assigns by default to the person exercising the highest authority within the enterprise,

may be delegated not only to an employee, but also to "**any person**" (s. 3.1(2) *in fine*[2]), *i.e*. **to a natural person working inside or outside the business.** This amendment allows businesses to outsource the function of privacy officer, in line with the approach taken in the European Union. Indeed, the Minister's comments when this amendment was tabled in Committee indicate that "this approach may allow for the use of services of a person specialized in the protection of personal information."

Policies and practices

The obligation for a business to publish its policies and practices relating to the governance of personal information on its website has been replaced by a more realistic obligation to publish "**detailed information about these policies and practices**" (s. 3.2(2)).

Privacy Impact Assessments

Following the introduction of Bill 64, several businesses expressed concern about the overreaching nature of the requirement to conduct a privacy impact assessment (PIA) with respect to ***any*** information system or electronic service delivery involving the collection, use, communication, keeping or destruction of personal information. The government has seemingly been attentive to the issue, considering that it has since amended that this obligation specifying that it only applies to the "**acquisition, development and redesign**" of a system (s. 3.3(1)). The parliamentary debates on this amendment allow us to draw two conclusions:

1. businesses will not be obliged to conduct PIAs with respect to existing systems when Bill 64 enters into effect; and
2. merely updating a system will not trigger the obligation to conduct a PIA unless the update introduces new functionalities that alter the way the system processes personal information.

This amendment also provides that 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**" (s. 3.3(4)). This precision suggests that a PIA will not be subject to any particular formalities or template. Moreover, it is interesting to see that the amendment invokes the same criteria as those provided for in section 10 of the Private Sector Act with respect to security measures. While it is easy to understand the connection between the sensitivity, the purpose, and the amount of personal information at issue and the PIA process, the notions of "distribution" and "format" need to be clarified. In our view, distribution can refer either to the physical location of the personal information (Is it stored on one or more servers? Where are these servers housed?). It may also point to its administrative status (How many people within the company and outside are authorized to access this information? Are these people working in one or more departments?) As for the format, it seems to refer to the material element on which the information is stored (*e.g.* a paper-based versus a technology-based document).

Privacy by design / by default

One of the provisions of Bill 64 that formalizes "privacy by design" is the new section 9.1, which requires businesses to ensure that, by default, the parameters of their technological product or service provide the highest level of confidentiality without any intervention by the person concerned. This section was amended in consideration of the provisions of the Access to Information Act to specify that:

1. it applies only to products and services that are offered to the public;
2. it applies only to products and services that have privacy parameters; and
3. it does not apply to the privacy settings of a cookie.

However, at the end of the parliamentary proceedings, **section 9.1 was suspended** by the Committee, thereby casting doubt on its adoption and, consequently, on its application to the private sector.

Consent and transparency

Transparency and confidentiality policy

An amendment was adopted requiring businesses to inform individuals of the "names of the third persons" to whom it is necessary to communicate the information for the purposes for which the information is collected (s. 8(2)). In our view, it would have been more realistic to include categories of third person, as permitted by the General Data Protection Regulation (GDPR). From a practical perspective, indicating the names of service providers would be of little use to individuals since they do not have a real choice to opt out of such transfers and since businesses remain responsible for the processing of personal information by their service providers. In consequence, this new requirement may contribute to information overload, which would be self-defeating in light of the Bill's transparency objective.

Moreover, there is uncertainty as to whether service providers are considered "third parties", given that the only provision of the Private Sector Act that deals with service providers is the new section 18.3 found in the *Communication to third persons* section of the Act. We therefore question how this requirement should be implemented, and whether it could be implemented at all, especially in a context where a business deals with a large number of service providers that may change over time.

New Consent Exceptions

While there has been some discussion about proposing a new general consent exception for legitimate business practices, the Committee has instead decided to add to section 12 two new narrow consent exceptions for specific uses of personal information. As a result, businesses will be able to use personal information without the consent of the individuals in the following five situations:

1. the use is necessary for the supply or the delivery of a product or the provision of a service requested by the person concerned (**new**); or
2. the use is necessary for the prevention and detection of fraud or the evaluation and improvement of protection and security measures (**new**);

3. the information is used in a manner consistent with the purposes for which it was collected, and there is a direct and relevant connection between the two (this exception will be particularly useful in the context of AI's training where the specific purposes of the processing may be difficult to identify at the time of the collection of data);
4. the information is clearly used for the benefit of the person concerned; and
5. the use is necessary for study or research purposes or for the production of statistics provided that the information is de-identified.

The two new exceptions (i.e. where the use is necessary for the supply or delivery of a product or for provision of a service requested by the person concerned and for the prevention and detection of fraud) seem to be comparable to some of the alternative legal bases for consent set out in the GDPR. These changes address situations in which the legitimate business practices of the company justify the processing of information, namely in instances of contractual necessity and in legitimate interests (GDPR, s. 6.1(b) and (f)).

Unfortunately, an amendment introducing an exception to consent for the use of personal information establishing, managing or terminating an employment relationship was not adopted . Given the difficulty of operationalizing a model of consent in the context of an employer-employee relationship; the Federal government, the government of British Columbia and the government of Alberta all recognize a clear exception to this effect in their private sector privacy legislation.

Bill 64 subtly introduces the notion of implied consent in sections 8, 8.3 and 12 of the Private Sector Act. As a result, employers could rely on the implied consent of employees to process their personal information if they provide all of the information required by section 8 and pursue a serious and legitimate purpose.

New obligations for the use of a technology with functions to identify, locate or profile an individual

An amendment replaced the word "deactivate" with the word "activate" in the second paragraph of section 8.1. This seemingly minor change has far-reaching consequences, **since it requires organizations that collect personal information using technologies that include functions allowing the person concerned to be identified, located or profiled to ensure that these functions are deactivated by default.** Indeed, Minister Eric Caire acknowledged in Committee that the purpose of this amendment was to introduce express consent for the collection of personal information through the use of technologies with identification, location or profiling features. It should be recalled that Bill 64 defines "profiling" broadly to include any collection and use of personal information to assess certain characteristics of a natural person (*e.g*. work performance, economic situation, health, personal preferences, interests or behaviour). This amendment therefore creates a great deal of uncertainty with respect to the use of online tracking tools such as cookies, beacons and pixels for marketing purposes since it is not clear if these technologies are covered by section 8.1. Should this turn out to be the case, the shift from an opt-out to an opt-in model would have serious implications for the entire digital advertising ecosystem by placing unfavourable conditions on Quebec-based businesses, in stark contrast to those applicable in the rest of Canada. It should also be noted that, even if online tracking tools are ultimately confirmed as falling within the scope of section 8.1, some of these tools do not include identification, localization or

profiling functions (e.g. cookies essential to the operation of a Web site) and would therefore potentially be exempt from this obligation.

Nevertheless, it is clear that express consent continued to be a requirement when the personal information collected is sensitive, as indicated in section 12, subsection 4 of the Private Sector Act. Moreover, an amendment was adopted to specify that **medical, biometric or otherwise intimate information** must be considered sensitive *by nature*, i.e. independently of its context of use. Thus, using a fingerprint or facial image to unlock a device or tracking a person's heart rate during physical activity are examples of the use of sensitive personal information that will require the express consent of the person concerned. It is unclear how the words "or otherwise intimate" will be interpreted, but this phrase will likely pave the way for various types of information (*e.g.*, financial, job performance, etc.) to be recognized as sensitive.

De-identification and anonymization

The Committee provided some clarification regarding two new concepts introduced by Bill 64, namely de-identification and anonymization of personal information. It is important to remember the distinction between these two concepts, which have very different scopes.

De-identified / pseudonymized information

Personal information is considered de-identified when it no longer allows the person concerned to be directly identified (section 12(4)(1)). In essence, this corresponds to the notion of "pseudonymized" information generally understood under the GDPR as the removal of all "direct identifiers"(e.g., name, social insurance number), while leaving "indirect identifiers" (e.g., date of birth, gender) intact. However, since de-identified information can still be used in combination with other information to identify a person, it remains subject to privacy legislation.

In this connection, an amendment to section 12 of the Private Sector Act introduces an obligation for enterprises that use de-identified information **to take reasonable steps to reduce the risks of anyone identifying a natural person using de-identified information** (s. 12(5)). It also bears mentioning that anyone who identifies or attempts to identify a natural person using de-identified information without the authorization of the person holding the information or using anonymized information commits an offence under the Act and is liable to a fine (s. 91(3)).

Anonymized information

Unlike de-identification, anonymization of personal information is excluded from the scope of the Private Sector Act. Thus, information concerning a natural person will be considered anonymized when 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** (s. 23(2)). The reference to "at all times reasonable to expect in the circumstances" is the result of an amendment adopted to require enterprises to ensure that their techniques for anonymizing personal information remain effective over time. Bill 64 provides that the anonymization of personal information must be carried out

according to “generally accepted best practices” and in accordance with criteria and procedures prescribed by regulation (s. 23(3)).

Anonymization of personal information is presented in Bill 64 as an alternative to its destruction. Accordingly, an enterprise that wishes to retain personal information beyond the preservation period will be able to do so provided that it anonymizes the information in order to use it **for a serious and legitimate purpose** (s. 23(1)). This condition of use for "a serious and legitimate purpose" was incorporated in response to the concerns of parliamentarians that anonymized information does not benefit from any restriction under the Private Sector Act. The "serious and legitimate reason" criterion set out in section 4 of the Private Sector Act with respect to the collection of personal information has therefore been adapted to this context to ensure that enterprises do not use anonymized information for purposes that a reasonable person would not consider acceptable in the circumstances. This new restriction on the use of anonymized information raises interpretative issues since anonymized information is technically excluded from the scope of the Private Sector Act (as it no longer constitutes personal information). It is difficult to see how the Act could impose specific conditions on the use of information that is excluded from its scope (and we note that such conditions do not exist under the GDPR).

Communication of personal information outside Québec

One of the most controversial provisions of Bill 64 pertains to the communication of personal information outside Québec. Several businesses have rightly criticized the new framework introduced in section 17 of the Private Sector Act. Essentially, this change established the unrealistic requirement that the legal framework applicable in the State to which the information would be transferred must offer a level of protection equivalent to the one afforded under the Private Sector Act. As such, Bill 64 would endow Québec with one of the world’s most stringent data protection regimes.

It is therefore fortunate that an amendment was adopted to remove the notion of jurisdictional equivalence from section 17 of the Private Sector Act. However, the conditions under which personal information may be communicated outside Québec (which includes another Canadian province, according to the Minister) remain highly restrictive. Before communicating personal information outside Québec, an enterprise must conduct a PIA which must take into account, among other things:

- the sensitivity of the information;
- the purposes for which it is to be used;
- 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*.

[Italics refers to the text added as a result of an amendment to Section 17]

The amendment further specifies that communication may occur if the PIA reveals that the personal information would receive an "**adequate**" (as opposed to "equivalent") protection in compliance with "**generally accepted data protection principles**." 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.

While section 17 no longer requires equivalent protection, assessing the legal framework applicable in the State in which the information would be communicated remains a factor to consider in the pre-disclosure PIA. In addition, section 17.1, which proposes the publication of a list of States whose legal data protection framework would be recognized as equivalent to that applicable in Québec by the government, was removed in the course of the Committee review.

In addition, the amendments made in Committee with respect to section 17 raise other sources of uncertainty for businesses, such as the notion of "generally accepted data protection principles", which is not defined in Bill 64 or in Québec legislation whatsoever. In our view, the broad wording of this notion suggests that a comprehensive data protection law, such as the Private Sector Act in Quebec, PIPEDA in Canada or the GDPR in the European Union, is not a prerequisite for the communication of personal information to a service provider located in a foreign State. Rather, businesses should assess the overall compliance of the foreign State's legal framework with the eight principles for the protection of personal information set out in the *OECD Privacy Guidelines* (originally adopted in 1980 and updated in 2013), namely:

1. Collection Limitation
2. Data Quality
3. Purpose Specification
4. Use Limitation
5. Security Safeguards
6. Openness
7. Individual Participation
8. Accountability

Additionally, the 2013 OECD guidelines also recognize whether a combination of adequate measures put in place by a data controller can ensure a continuous level of protection. These include technical and organisational security safeguards, contracts, complaint handling processes, and audits (provided these can be supplemented by effective enforcement if these measures prove ineffective). Despite the amendments made in the Committee, the framework provided by section 17 of the Private Sector Act for the communication of personal information outside Québec remains very restrictive, which may result in significant operational costs for enterprises operating in Québec. The government could have achieved the same objective, *i.e.* to safeguard the personal information of Quebecers when it is transferred abroad, by requiring businesses to enter into a data protection agreement that includes standard clauses when information is transferred outside Quebec, similar to what is actually provided in the EU.

New Enforcement Mechanisms

To date, no amendments have been made to the new enforcement mechanisms applicable to the private sector, as the provisions of Bill 64 to this effect had not yet been considered by the parliamentary committee at the end of its session. It is worth recalling the three mechanisms provided by Bill 64 to ensure compliance by enterprises with the Private Sector Act, namely:

- **Monetary administrative penalties** imposed by the Commission d'accès à l'information;
- **New penal offences** with significant fines; and
- The **right to sue** an enterprise for damages caused by an unlawful infringement of a right conferred by the Private Sector Act or by articles 35 to 40 of the Civil Code, and to obtain punitive damages if the infringement is intentional or results from a gross fault.

Next Steps

Assuming that Bill 64 review will proceed when the National Assembly reconvenes in September, it is reasonable to expect that the Bill could be passed by December 2021. Thus, subject to the right to data portability, which is subject to a 3-year effective period, the provisions of Bill 64 would take effect one year after its adoption, potentially in the last two quarters of 2022.

With Bill C-11 deadlocked in the House of Commons, Québec is in the process of becoming the first jurisdiction in Canada to modernize its privacy legislation in light of international precedents, such as the GDPR in Europe and the *California Consumer Privacy Act of 2018* (CCPA) in the United States. While we can only applaud Québec's proactivity, the risk of a lack of regulatory harmonization in Canada is real and is certainly a significant concern for enterprises.

Ultimately, despite the amendments made to Bill 64 in Committee (and sometimes because of them), several amended provisions of the Private Sector Act are likely to cause major challenges for businesses, including:

- The interpretation and application of the PIA "proportionality" test;
- The uncertain fate of section 9.1 on privacy by design/by default;
- The absence of an exception to consent for the use of personal information establishing, managing or terminating an employment relationship;
- The requirement to deactivate "by default" technologies that identify, locate or profile a person when used to collect personal information;
- The requirement to inform individuals of the names of third persons to whom an organization may communicate personal information;
- The limitation on the use of anonymized information to "a serious and legitimate purpose"; and
- The regime for the communication of personal information outside Québec, which remains overly demanding and unrealistic.

Although not discussed in this article as the relevant provisions were passed without amendments, the Committee proceedings raised new concerns about the following three issues:

- The notion of "separate" and "granular" consent remains difficult to interpret in the absence of specific guidance; and
- The application of the new data portability right to inferred data, *i.e.*, information that a business has deduced or derived from the personal information provided by the person concerned (*e.g.*, his or her preferences in some products or services). While the government had clearly excluded this possibility in a brief filed at the introduction of Bill 64, recent statements by Minister Caire made in

Committee seem to indicate that the right to portability would apply to any information relating to a person and allows the person to be identified, whether inferred or not.

Several new provisions introduced by Bill 64 may require substantial operational changes to be implemented. Many of them raise some uncertainty about their interpretation; many businesses are hopeful that the government will introduce an extended transition period (perhaps eighteen months or ideally even two years). At the very least, the government could consider delaying the enforcement provisions, including the monetary administrative penalties, new penal offences and private right of action. If nothing else, it would be beneficial to provide a limited maintenance of "acquired rights" with a sunset provision so that businesses have enough time to modify and adjust their current business practices before these provisions come into effect.

We are currently working on a practical guide to help businesses comply with the new requirements introduced by Bill 64. This guide will be made public once the final and definitive version of Bill 64 is adopted. In the meantime, please do not hesitate to contact BLG's Privacy and Data Protection team if you have any questions about recent developments concerning the protection of personal information in Quebec.

[1] Please note that in this amended version, the text in red reflects the modifications made by Bill 64 to the Private Sector Act, while the text in blue represents the amendments adopted to Bill 64 by the Committee.

[2] Unless otherwise indicated, the sections cited in this bulletin refer to the Private Sector Act as amended by the provisions of Bill 64.

Special thanks to Simon Du Perron for his contributions to this publication.

By

Elisa Henry, Max Jarvie, Andy Nagy, Simon Du Perron

Expertise

Cybersecurity, Privacy & Data Protection, Compliance with Privacy & Data Protection, Data Mapping & Gap Analysis, Personal Health Information & Privacy, Corporate Commercial

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 725 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