BILL 64: MODERNIZING QUÉBEC'S PRIVACY REGIME

Posted on July 23, 2020

Categories: Insights, Publications

On June 12th, the National Assembly (Québec) unanimously voted to table Bill 64, entitled "*An Act to modernize legislative provisions as regards the protection of personal information*", submitted by the former Minister of Justice, Sonia Lebel, now Minister Responsible for Democratic Institutions, Electoral Reform and Access to Information.

As its name suggests, this Bill would modernize Québec's private and public sector privacy regimes to ensure that the legislative framework for the protection of personal information is better adapted to present-day realities and keeps pace with the international legislative framework. In this Bulletin, we will deal only with the amendments to the *Act respecting the protection of personal information in the private sector* (CQLR c. P-39.1) (the "Act"), which has been in force since 1994, and of which the last significant amendments date back to 2006.

This Bill (1) adds new obligations for companies doing business in Québec; (2) addresses several shortcomings of the Act; and (3) makes companies more accountable through new and increased penalties.

1. New Obligations

- Privacy Policy

If not already done, organizations will have to establish and implement policies and practices that are proportional to the nature and extent of their activities, which structure their governance regarding personal information and the protection of such information. These policies shall namely provide for measures regarding the protection and destruction of personal information, the roles and responsibilities of their staff members throughout the information life cycle, and the implementation of a complaints processing method. These policies and practices must be approved by the person in charge of the protection of personal information and should be published on the organization's website.[1]

In addition, all organizations which gather personal information using technological means shall now have to publish on their websites and disclose by any means appropriate to reach the persons concerned, a privacy policy written in clear and simple terms. This includes technologies whose functions allow for the identification, location, or profiling of persons, such as the use of cookies or targeting technologies. Organizations must give

prior notice to their users that they are using such technologies and instructions on how to deactivate functions that allow the user to be identified, located, or profiled. Organizations must also notify their users of any amendment to this policy. Note that the term "technology" would encapsulate mobile devices and applications, as well as services dependent on individual-based metrics such as recommendation engines (e.g., streaming media services). It would be prudent in connection with all of these services to make the privacy policy (and any related amendment) available not only on the organization's website but also in the application and/or by email.[2]

- Privacy Impact Assessment

Borrowing from the E.U. regulation No. 2016/679, entitled *General Data Protection Regulation* ("**GDPR**"), Bill 64 introduces the obligation to conduct a privacy impact assessment of each information system project or electronic service delivery project involving personal information, and to implement privacy by design measures. The latter includes an obligation to consult with the person in charge of the protection of personal information from the outset of the project.[3]

- Appointment of a Privacy Officer

The privacy officer is tasked with ensuring that the organization implements and complies with the obligations imposed by the Act. This duty falls on the person exercising the highest authority in the organization, though it may be delegated in writing, in whole or in part, to a staff member. The title and contact information of the person in charge of the protection of personal information (i.e., the privacy officer) must be posted on the organization's website.[4] The privacy officer will be responsible for addressing access to information requests, requests for the correction of personal information, and questions or complaints concerning the handling of personal information.

- Confidentiality Incident / Privacy by Default

As soon as an organization has reason to believe that a confidentiality incident has occurred involving personal information that it holds, it will be required to take reasonable measures to reduce any risk of prejudice and to prevent similar incidents from occurring. A confidentiality incident is defined as access to, use, or communication of personal information not authorized by law, as well as the loss or any infringement of the protection of such information. In comparison to other Canadian privacy laws, this stricter definition broadens the scope of what constitutes a confidentiality incident to include the unauthorized use of personal information, thereby exceeding the scope of other Canadian data breach notification requirements.

Every confidentiality incident must be logged by the organization in a register of confidentiality incidents. In case of a risk of serious prejudice, the organization must promptly notify the *Commission d'accès à*

l'information ("**CAI**") [Access to Information Commission], as well as any person whose personal information is concerned by the incident. The organization may also — without obligation to obtain consent of the person concerned — notify any person or body who or which is likely to reduce the risk of prejudice (e.g., credit institutions) by disclosing only necessary personal information, except when this would be likely to obstruct an investigation conducted by a person or an organization tasked with preventing, detecting, or suppressing crime or statutory offences.[5] The reporting threshold of a "risk of serious injury" appears to correspond to the reporting threshold of a "real risk of significant harm" under the *Personal Information Protection and Electronic Documents Act,* (S.C. 2000, ch. 5) ("**PIPEDA**").

Lastly, the Bill introduces the concept of the "highest level of confidentiality by default" (i.e., privacy by default), requiring that the parameters of a technological product or service be established by default, without user intervention, at the highest confidentiality level. This provision reflects the recent debate on the necessity of establishing stricter privacy parameters by default in social media and other online services. A similar privacy by default obligation exists in GDPR.[6]

- Consent

There are also several new rules regarding consent. For consent to be valid, the Bill requires that requests for consent regarding the collection or handling of personal information must be sent in simple and clear terms to the person concerned, no matter what means are used to collect the information, and independently from any other information disclosed to that person.[7]

In addition, the personal information collected may be used only within the organization for the purposes for which it was initially collected, and if such purposes change, the consent of the person concerned must be obtained once again.[8]

Nevertheless, it would be possible to use personal information for another purpose without the consent of the person concerned when such use is (i) for purposes consistent with those for which it was collected (meaning that there must be a direct and relevant connection with the initial purpose, while commercial or philanthropic prospection will not be considered a consistent purpose); (ii) clearly for the benefit of the person concerned; or (iii) necessary for study or research purposes, or for the production of statistics, and where the information is de-identified (when it is no longer possible to directly identify the person concerned by the information).[9] However, the Bill would cancel any right the organization may have had under the Act to disclose to third parties nominative lists (i.e., contact lists) without the consent of the persons concerned.[10]

Another new rule would require that consent be expressly given when sensitive personal information is concerned. The notion of sensitive personal information is introduced in the Act to include information, which

due to its nature or the context of its use or communication, entails a high level of reasonable expectation of privacy.[11]

Regarding "consent" itself, the Bill recharacterizes consent as being "*clear, free, and informed and [...] given for specific purposes,*" which has slightly changed from "*manifest, free, and enlightened, and [...] given for specific purposes.*"[12] This is in line with the Office of the Privacy Commissioner of Canada ("OPC") guidelines for meaningful consent, and to a greater extent, very similarly worded to the meaning of consent under GDPR: *"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement [...]."*[13]

Lastly, when the collection, use, or communication of information concerns minor persons of less than 14 years old, the consent of the person having parental authority would be required, unless collecting the information is clearly for the minor's benefit. The consent of a minor person of 14 years and older may be given by that minor person, or by the person having parental authority.[14]

- Making Decisions Regarding Persons Concerned

The Bill introduces a new obligation regarding the storing of personal information and requires that any personal information used to make a decision regarding the person concerned be kept for at least one year following the decision.[15]

On the other hand, when a decision is exclusively based on the automated processing of collected personal information, the Bill adds an obligation of transparency. Increasingly, technologies are being tasked to render decisions based on personal information (e.g., AI-based decision-making). When such a decision is made, the organization would be required to first notify the person concerned, and then make available to that person on request, additional information concerning the decision-making process, namely, the reasons and parameters that led to the decision.[16] This transparency requirement seems to stem from GDPR, but does not go as far as the latter regulation in granting the data subject, in certain cases, the right to withdraw from being the subject of a decision made exclusively by automated processing.

- Communication of Information Outside of Québec

One of the Bill's most far-reaching provisions is the requirement that the cross-border communication of personal information be preceded by an informal assessment of privacy protection, taking into consideration a number of factors, namely: (i) the sensitivity of the information; (ii) the purposes for which it is to be used; (iii) the safeguards that would apply to it; and (iv) the legal framework applicable in the jurisdiction to which the information would be communicated. This requirement would apply to the processing of information outside of Québec, including storage and hosting.[17]

Even though the Bill had been tabled before the recent judgment of July 16, 2020, by the European Union Court of Justice in the case known as *Schrems II* (C-3111/18), parallels may be established between the case-by-case assessment required under the Québec Bill and the case-by-case assessment required under GDPR for the cross-border transmission of data to/from Europe under standard contractual clauses. Likewise, Québec would systematically assess the legal frameworks of foreign jurisdictions to determine the "degree of equivalency" to Québec's protection of privacy principles, which is very similar to the concept of "adequacy" of foreign jurisdictions for cross-border data flows. However, according to the current wording of the Bill, an organization would likely still need to conduct an informal assessment of the protection of privacy even if the destination jurisdiction is considered to be "equivalent" under Québec standards.

2. Shortcomings Remedied

In general, the new obligations in the Bill reflect privacy provisions already in force in most of Canada, either under PIPEDA or pursuant to recommendations made by the OPC. The Bill is more stringent, however, in making some of its new provisions compulsory, and not merely making strong recommendations as does PIPEDA.

In addition, the Bill removes obscure terminologies from the Act, using more widely accepted language. It replaces "file" with "personal information" and "object of the file" with "purpose".

- Business Contact Information

Section 1 of the Act would be amended to extend the public information exception (to which Divisions II "*Collection of Personal Information*" and III "*Confidentiality of Personal Information*" of the Act do not apply) to also exempt business contact information. Business contact information refers to information that relates to the performance of a person's business functions within an organization, such as name, title, and duties, as well as physical address, email address, and telephone number of their place of work. Accordingly, business contact information would be exempt from requirements regarding the collection and handling of personal information, as is currently the case under PIPEDA, the *Personal Information Protection Act* (S.A. 2003, C. p-6.5) of Alberta ("**Alberta PIPA**") and the *Personal Information Protection Act* (S.B.C. 2003, c.63) of British Columbia ("**BC PIPA**").[18]

- Communications for the Exercise of Functions or the Performance of a Mandate or a Contract

The Bill also strengthens regulation of the existing exception concerning communications for the purposes of a mandate or a contract (which allows for the communication of personal information to third parties to the extent the information is necessary to carry out a mandate or perform a contract of enterprise or for services, without having to obtain additional consent of the person concerned) by enacting more stringent

requirements. These include the need to contractually specify safeguards, limits on use, and retention limits, as well as to notify of security incidents and allow the auditing of protective measures. Note that these requirements will not apply when the mandatary or the person performing the contract is a public body within the meaning of the Act respecting Access to documents held by public bodies and the Protection of personal information (CQLR c A-2.1) or a member of a professional order.[19]

- Commercial Transactions

The Bill specifies that personal information that is necessary to conclude a commercial transaction involving the transfer of ownership of all or part of an organization may be communicated to the other party to the transaction without the consent of the persons concerned. It sets out that an agreement must be entered into with the other party prior to the communication, stipulating that that party must (i) use the information only for concluding the commercial transaction; (ii) not communicate the information without the consent of the person concerned; (iii) take the measures required to protect the confidentiality of the information; and (iv) destroy the information if the commercial transaction is not concluded, or if using the information is no longer necessary for concluding the commercial transaction. Once the commercial transaction is concluded, the other party may continue to use or communicate the personal information only in compliance with the Act, and must notify the persons concerned within a reasonable time limit that it now holds personal information concerning them in connection with the transaction. This amendment to the Act would bring it in line with PIPEDA, Alberta PIPA, and BC PIPA.[20]

- Study, Research, or Statistics

Organizations wishing to receive personal information for study, research or statistical purposes would no longer be required to obtain authorization from the CAI or obtain the prior consent of the persons concerned. Under the Bill, organizations may communicate personal information without prior consent, to any person or body who or which intends to use it for such purposes, subject to an assessment of privacy factors by the organization that reaches the following conclusions: (i) the objective of the study or research or of the production of statistics can be achieved only if the information is communicated in a form allowing the persons concerned to be identified; (ii) it is unreasonable to require the person or body to obtain the consent of the persons concerned; (iii) the objective of the study or research or of the production of statistics outweighs the impact, of communicating and using the information, on the privacy of the persons concerned; (iv) the personal information is used in such a manner as to ensure confidentiality; and (v) only the necessary information is communicated.[21]

- Portability/Right to be Forgotten

In addition to a right of access, individuals would have a right to data portability, similar to what is provided under GDPR. The Bill provides that a person may request that his/her/their information be communicated or transferred to another body in a structured and commonly used format.[22]

Individuals would also have the right to demand that their personal information be de-indexed or otherwise ceased from being disseminated, under certain circumstances. In an online, search-based world, this is tantamount to a right to be forgotten and appears to be inspired by a related right provided under GDRP.[23]

3. Deterrent Measures

The implementation of new deterrent measures would focus on the protection of individuals and accountability of organizations.

While currently, complaints can be filed only by the interested parties, the Bill would allow the CAI to undertake investigations on the basis of anonymous complaints.[24] In addition, new whistle-blower protections for persons who file a complaint in good faith with the CAI or co-operate in an investigation, would prohibit reprisals and threats of reprisals against current or prospective complainants.[25]

A far cry from the maximum penalty of $10,000 for an offence under the Act, or of $50,000 for communicating information outside of Québec contrary to the Act, organizations would now face the risk of being fined from $15,000 to $25,000,000 or 4% of their worldwide turnover for the preceding fiscal year if this last amount is greater. Such fines could be imposed where an organization (i) collects, holds, communicates to third persons, or uses personal information in contravention of the Act, (ii) fails to report, where required to do so, a confidentiality incident to the Commission or to the persons concerned, (iii) 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, or (iv) impedes the progress of an inquiry or inspection of the CAI. These amounts would be doubled for subsequent offences.[26] For physical persons, directors, officers or representatives of a body who are vicariously responsible for an offence, whether by ordering, authorizing, or consenting to the act or omission in question, the penalty in force would increase five-fold from $10,000 for most offences to $50,000.

In addition, new administrative penalties would be administered by the CAI, as part of its new supervisory powers for enforcement of the Act. It may also undertake statutory prosecutions for any offence under Division VII "*Application of this Act*". Monetary administrative sanctions would be a maximum of $10,000,000 or 2% of the organization's worldwide turnover for the preceding fiscal year if this last amount is greater.[27] The CAI would become the first Canadian privacy regulatory body with the power to impose administrative monetary sanctions for non-compliance with privacy laws.

Lastly, the Bill grants a private right of action for damages resulting from the unlawful infringement of the right to privacy conferred by the Act or by articles 35 to 40 of the Civil Code of Québec. When such an infringement is intentional or results from a gross fault, the victim would be entitled to punitive damages of at least $1,000.[28] Such a private right of action would undoubtedly contribute to an increase of privacy-related class actions.

4. Conclusion

Because Bill 64 is in first reading, it may be amended before being adopted by the National Assembly and sanctioned by the Lieutenant Governor. If the Bill is enacted, it will probably not come into force before a period of one year from the date of its assent, that is, the fall of 2021 at the earliest.

Revision of Québec's privacy legislation has been anticipated for a long time. This modernization would arguably make Québec's privacy regime the strictest on this side of the Atlantic. In addition to aligning the province's legislation with other Canadian legislation (e.g., PIPEDA), the proposed amendments in Bill 64 would make it more consistent with international privacy protection standards (e.g., GDPR).

In June 2014, the G29 or "Article 29 Data Protection Working Party" presented an opinion to the European Commission, holding that Québec's privacy legislation was not "adequate", as measured against European standards, for the purposes of cross-border transmission of personal information between Québec and Europe. Although PIPEDA has "adequate" status for the transmission of data governed by GDPR, the same does not apply to Québec. Proposed revisions provided in this Bill may help Québec obtain "adequate" status, allowing for the unfettered transmission of data between Québec and Europe, even if some key points are still missing, namely regarding the exception to consent for the collection, use or communication of personal information required for managing an employment relationship. Likewise, this Bill takes a one-size-fits-all approach, although a more progressive approach to compliance obligations based on the size of the organization would arguably be more practical.

In addition, as modernized by the Bill, enforcement of the Act would likely be difficult at the outset, including a potential deluge of data breach notifications, as has occurred elsewhere in Canada and Europe. Accordingly, organizations operating in Québec may expect the Québec privacy watchdog to increase in size and budget.

We will monitor this Bill closely and keep you posted on any new developments. In the meantime, to remain ahead of the game regarding any coming compliance obligations, organizations operating in Québec should consider the following:

- Review their privacy policy and practices regarding consent;
- Review their upstream and downstream contractual obligations regarding the protection of personal

information;

- Conduct a data audit/mapping to determine cases where appropriate consent could be missing;
- Implement a consent management system;
- Implement or revise retention and incident response policies and procedures; and
- Evaluate existing physical, organizational and technological privacy safeguards.

It would be a pleasure to assist you with any questions regarding the privacy laws in Québec or in the rest of Canada, as well as with any issues you may have regarding your compliance initiatives.

by Candice Hévin and Rish Handa

[1] Section 95 of Bill 64, which adds a new division to the Act, entitled "*Responsibilities Relating to Protection of Personal Information*", comprising new sections 3.1 to 3.8.
[2] Section 99 of Bill 64, which adds the new sections 8.1 to 8.3 to the Act.
[3] Section 95 of Bill 64, which adds the new sections 3.3 and 3.4 to the Act.
[4] *Supra* note 1, section 3.1.
[5] Section 95 of Bill 64, adding the new section 3.5 to the Act.
[6] Section 100 of Bill 64, adding the new section 9.1 to the Act.
[7] Section 102 of Bill 64, amending section 14 of the Act.
[8] Section 102 of Bill 64 amending section 12 of the Act.
[9] *Ibid*.
[10] Section 104 of Bill 64, amending section 18 of the Act.
[11] *Supra* note 8.
[12] Section 102 of Bill 64, amending section 14 of the Act.
[13] Article 4(11) of GDPR.
[14] Sections 96 and 102 of Bill 64, adding the new section 4.1 to the Act and amending section 14.
[15] Section 101 of Bill 64, amending section 11 of the Act.
[16] Section 102 of Bill 64, adding the new section 12.1 to the Act.
[17] Section 103 of Bill 64, amending section 17 and adding section 17.1 to the Act. .
[18] Section 93 of Bill 64, amending section 1 of the Act.
[19] Section 107 of Bill 64, adding the new section 18.3 to the Act.
[20] Section 107 of Bill 64, adding a new section 18.4 to the Act.
[21] Section 110 of Bill 64, adding the new section 21 to the Act.
[22] Section 112 of Bill 64, amending section 27 of the Act.
[23] Section 113 of Bill 64, adding a new section 28.1 to the Act.
[24] Section 143 of Bill 64, amending section 81 of the Act.

[25] Section 144 of Bill 64, adding a new section 81.1 to the Act.
[26] Section 151 of Bill 64, adding new sections 91 to 92.2 to the Act.
[27] Section 150 of Bill 64, adding new sections 90.1 to 90.17 to the Act.
[28] Section 152 of Bill 64, adding a new section 93.1 to the Act.

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.