BILL 64 ENACTED: QUÉBEC'S MODERN PRIVACY REGIME

Posted on October 15, 2021

Categories: Insights, Publications

On September 21st, the National Assembly of Québec unanimously voted to pass Bill 64, an *Act to modernize legislative provisions as regards the protection of personal information*, and the bill received assent the following day.

The result is that Québec has significantly modernized its private and public sector privacy regimes, better adapting its legislative framework for the protection of personal information to present-day realities and keeping pace with international privacy developments. In this Bulletin, we will deal only with the amendments to the *Act respecting the protection of personal information in the private sector* (the "**Act**"), which has been in force since 1994, and of which the last significant amendments date back to 2006. We will also outline the key changes to Bill 64 made during the parliamentary review process since the bill was originally proposed in June 2020.

The amendments add new obligations for organizations doing business in Québec, address several shortcomings of the previous version of the Act, and add new and stringent enforcement mechanisms. Many of the new obligations reflect privacy provisions already in force in most of Canada, either under the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") or pursuant to recommendations made by the Office of the Privacy Commissioner of Canada ("**OPC**"). However, the reforms are backed by stringent enforcement measures, rather than merely strong recommendations as is the case under PIPEDA.

The new private-sector requirements will come into effect in three phases over the course of the next three years. The requirement to appoint a Privacy Officer and the breach notification requirements will take effect as of September 22, 2022. The majority of the new requirements will take effect as of September 22, 2023. And finally, the data portability right will take effect as of September 22, 2024.

1. New Obligations as of 2022

Appointment of a Privacy Officer

Organizations are now required to appoint a person in charge of the protection of personal information ("**Privacy Officer**"). Specifically, the Privacy Officer is tasked with ensuring that the organization complies with the obligations imposed by the Act and 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. By default, this duty falls on the person exercising the highest authority in the organization (e.g., the CEO), though it may be delegated in writing, in whole or in part, to any person (internally or externally). Under the original language of Bill 64, the duty could only be delegated internally (e.g., to a staff member), but this restriction was amended in parliamentary committee, allowing organizations to outsource this responsibility to a qualified, external professional advisor. The title and contact information of the Privacy Officer must be posted on the organization's website.[1]

Breach Reporting

As soon as an organization has reason to believe that a confidentiality incident has occurred involving personal information in its custody, it must take reasonable measures to reduce any risk of harm 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.

In case of a risk of serious injury, 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 third party that is likely to reduce the risk of harm (e.g., credit institutions) by disclosing only necessary personal information, except when this would be likely to obstruct a law enforcement or regulatory investigation. The reporting threshold of a "risk of serious injury" appears to correspond to the reporting threshold of a "real risk of significant harm" under PIPEDA, in that the organization must consider the sensitivity of the information concerned, the anticipated consequences of its use, and the likelihood that such information will be used for harmful purposes. Every confidentiality incident must be logged by the organization in a register of confidentiality incidents, which must be provided to the CAI upon request.[2]

Once the new enforcement provisions take effect in late 2023, the CAI will be able to order any person involved in a confidentiality incident to take any measure to protect the rights of persons concerned, for the time and on the conditions the CAI determines. In particular, the CAI may order that the personal information involved be returned to an organization (e.g., data controller or breached organization) or destroyed.[3]

Commercial Transactions

Personal information necessary to conclude a commercial transaction (i.e., in the context of M&A or a financing) may be communicated to another party to the transaction without the consent of the persons concerned. The

parties must enter into an agreement prior to the communication, stipulating that the receiving 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 receiving 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 period that it now holds personal information concerning them in connection with the transaction. This amendment brings the Act's approach to commercial transactions in line with PIPEDA, the *Personal Information Protection Act* of Alberta ("**Alberta's PIPA**"), and the *Personal Information Protection Act* of British Columbia ("**BC's PIPA**").[4]

Study, Research, or Statistics

Organizations wishing to receive personal information for study, research or statistical purposes will no longer be required to obtain authorization from the CAI or obtain the prior consent of the persons concerned. Under the reformed Act, 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, in light of the public interest, 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. In addition, the organizations sharing the personal information must first enter into an agreement containing prescribed information to ensure the protection of the personal information involved, and the agreement must be sent to the CAI a month prior to the sharing of the information.[5]

2. New Obligations as of 2023

Privacy Framework

Organizations will have to establish and implement a privacy framework comprising policies and practices that are proportional to the nature and extent of the organization's activities, to ensure the protection of personal information. These policies shall namely provide for measures regarding the protection and destruction of personal information, the roles and responsibilities of staff members throughout the information life cycle, and the implementation of a process to handle complaints. The privacy framework must be approved by the

Privacy Officer. Further, the organization must publish on its website, in clear and simple language, detailed information about these policies and practices.[6]

Transparency

Under the reformed Act, individuals are afforded much more transparency as to how their personal information is to be handled. Accordingly, organizations have numerous disclosure obligations, including (i) the purposes for which personal information is collected, (ii) the means by which the information is collected, (iii) rights of access and rectification, (iv) the person's right to withdraw consent to the communication or use of the information, (v) whether there is the possibility that the information may be communicated outside Québec, and (vi) the names of the third parties or categories of third parties to whom it is necessary to communicate the information for the purposes set out. This last element, which was added during parliamentary review of Bill 64, is likely to cause organizations the most angst, as the identities or classes of third-party processors are not always known at the time personal information is initially collected.[7]

In addition, all organizations that gather personal information using technological means shall now have to publish on their websites and disclose by any means appropriate in order to reach the persons concerned, a privacy policy written in clear and simple terms. This includes technologies whose functions allow for the identification, locating, or profiling of persons, such as the use of certain cookies or targeting technologies. Organizations must give prior notice to their users that they are using such technologies and instructions on how to activate 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" in this context 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.[8]

During parliamentary review, the language of Bill 64 was changed from requiring instructions on how to "deactivate" functions that allow for the identification, locating, or profiling of persons, to how to "activate" them, reflecting a requirement that such functions be deactivated by default. This obligation may prove to be a significant burden on organizations, particularly where such functions are critical to the intended use of a product or service.

Privacy Impact Assessments

Borrowing from E.U. regulation No. 2016/679, entitled *General Data Protection Regulation* ("**GDPR**"), the Act

obligates organizations to conduct a privacy impact assessment of each project of acquisition, development, and redesign of an information system or electronic service delivery involving personal information, and to implement privacy by design measures. The latter includes an obligation to consult with the Privacy Officer from the outset of the project. The Privacy Officer may at any stage of the project suggest the implementation of applicable safeguards (e.g., the appointment of a project-based privacy manager, privacy training, or measures to protection personal information). In addition to the restriction of privacy impact assessments to projects of "acquisition, development, and redesign", the language of Bill 64 was also amended to require assessments to be proportionate to the sensitivity of the information involved, its intended uses, and the amount, distribution, and format of the information.[9]

Privacy by Default

The Act now incorporates the concept of "highest level of confidentiality by default" (i.e., privacy by default), requiring that the parameters of a public-facing technological product or service that has privacy parameters be set by default (i.e., 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. Notably, the language originally proposed under Bill 64 was revised in committee to restrict the privacy by default requirement to (i) products and services that are offered to the public, as opposed to internal business technologies; (ii) products and services that have privacy parameters; and (iii) exclude cookies, as cookies themselves do not have customizable privacy settings.[10]

Consent

There are several new rules regarding consent. Importantly, where an organization meets its disclosure requirements at the time of collection of personal information, the provision of the information is deemed a consent to its use and communication for the purposes set out in the disclosure. When a request for consent is required, such as where sensitive personal information is concerned, for such consent to be valid, the reformed Act requires that the request be made in simple and clear terms, and if made in writing, must be presented independently from any other information disclosed to the person.

Further, the reformed Act 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*."[11] This is in line with the OPC guidelines for meaningful consent, and to a greater extent, is 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 [...].*"[12]

In addition, personal information collected may be used within the organization only for the purposes for which it was initially collected. If additional use cases arise, except for the scenarios enumerated below, additional consent of the person concerned must be obtained.[13]

It will 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, though commercial or philanthropic prospection is not considered a consistent purpose); (ii) clearly for the benefit of the person concerned; (iii) necessary for the prevention and detection of fraud or the evaluation and improvement of protection and security measures; (iv) necessary for the supply or delivery of a product or the provision of a service requested by the person concerned; or (v) necessary for study or research purposes, or for the production of statistics, where the information is de-identified (i.e., when it is no longer possible to directly identify the person concerned by the information). Exceptions (iii) and (iv) above were added during parliamentary review. In contrast to the new exceptions to consent, the reforms to the Act remove any explicit right the organization previously had to disclose to third parties nominative lists (i.e., contact lists) without the consent of the persons concerned.[14]

As indicated above, the reformed Act requires that consent be expressly given when sensitive personal information is concerned, bringing the Act in line with regulatory guidance. Sensitive personal information is information which, due to its nature or the context of its use or communication, entails a high level of reasonable expectation of privacy, including medical, biometric, or otherwise intimate information.[15]

Lastly, when the collection, use, or communication of information concerns minors of less than 14 years old, the consent of a person with parental authority is required, unless collecting the information is clearly for the minor's benefit. The consent of a minor of 14 years and older may be given by the minor, or by a person having parental authority.[16]

Making Decisions Regarding Persons Concerned

The reforms introduce a new retention obligation, requiring that any personal information used to make a decision regarding the person concerned be kept for at least one year following the decision.[17]

When a decision is based exclusively on the automated processing of collected personal information, the reforms add a new disclosure obligation to promote 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 is required to notify the person concerned that the decision was based exclusively on an automated processing of personal information, and upon request, make available additional information concerning the decision-making process, namely, the reasons and parameters that led to the decision.[18] 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 more far-reaching reforms 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 protection measures (including contractual) that would apply to it; and (iv) the legal framework applicable in the jurisdiction to which the information would be communicated, including the data protection principles applicable in the jurisdiction. This requirement would apply to the processing of information outside of Québec, including storage and hosting.[19]

Even though Bill 64 had been tabled before the landmark ruling by the European Union Court of Justice regarding cross-border transmissions in the case known as *Schrems II* (C-3111/18), in July 2020, parallels may be established between the case-by-case assessment required under the Act and the case-by-case assessment required under GDPR for the cross-border transmission of data to/from Europe under standard contractual clauses. While Bill 64 originally envisaged the systematic assessment of the legal frameworks of foreign jurisdictions to determine the "degree of equivalency" to Québec's privacy principles in the context of cross-border data flows, this equivalency regime was scrapped during parliamentary review in favour of assessing whether communicated information would receive adequate protection in compliance with generally accepted data protection principles. Nevertheless, an organization must conduct an informal privacy protection assessment for any communication of personal information outside of Québec, regardless of the destination jurisdiction.

Business Contact Information

The Act has been 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 will be exempt from requirements regarding the collection and handling of personal information, as is currently the case under PIPEDA, Alberta's PIPA, and BC's PIPA.[20]

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

Under the reformed Act, there are additional obligations when communicating personal information to a third party (e.g., service provider) 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. The new obligations include the need to contractually specify safeguards, limits on use, and retention limits, as well as for the third party 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.[21]

Right to be De-indexed

Individuals will 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 GDPR.[22]

Anonymized Data

Of great importance to many organizations is the ability to retain data, in some form or another, once the applicable retention period under privacy law concludes. The reforms to the Act provide some guidance in this respect. Once the purposes for which personal information was collected or used are achieved, generally, the organization must destroy the information or anonymize it in order to use it for a serious and legitimate purpose. Information is deemed "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. Further, the anonymization process must comply with generally accepted best practices as well as criteria and procedures prescribed by regulation (which has not yet been implemented).[23]

3. New Obligations as of 2024

Right to Data Portability

In addition to a right of access, individuals will have a right to data portability, similar to what is provided under GDPR. The Act provides that a person may request that their personal information be communicated or transferred to the person or a third-party organization in a structured and commonly used format. The right is limited in two respects: (i) it does not cover information created or derived from collected personal information, and (ii) the right does not extend to instances that raise serious practical difficulties. The former limitation was introduced during committee, permitting organizations to only return personal information collected from the person, without having to share any proprietary data.[24]

4. Enforcement

The Act will be enforceable under new investigative and enforcement mechanisms: (i) reformed complaint and investigative procedures, (ii) administrative monetary penalties (AMPs), (iii) penal offences with significant fines, and (iv) a private right of action. The new enforcement regime will largely take effect as of September 2023, though certain of the new complaint and investigative procedures will take effect as of September 2022.

While currently, complaints can be filed only by interested parties, the CAI will soon be able to undertake investigations on the basis of anonymous complaints.[25] In addition, new whistle-blower protections for persons who file a complaint in good faith with the CAI or co-operate in an investigation will prohibit reprisals and threats of reprisals against current or prospective complainants.[26]

As part of its new supervisory powers for enforcement of the Act, the CAI will be able to directly impose administrative monetary penalties ("**AMPs**") for certain violations. Such **administrative monetary penalties can reach up to the greater of $10,000,000 or 2% of the organization's worldwide turnover** for the preceding fiscal year. The types of violations that may attract an AMP include where an organization: (i) fails to meet its transparency obligations at the time of collection of personal information; (ii) collects, uses, communicates, holds, or destroys personal information in contravention of the Act; (iii) fails to report a confidentiality incident to the CAI or to the persons concerned, where required to do so; (iv) fails to implement appropriate safeguards to protect personal information; or (v) fails to adequately inform the person concerned about a decision based exclusively on an automated process or allow the person to submit comments to assist a review of the decision.[27]

The CAI will become the first Canadian privacy regulatory body with the power to impose administrative monetary sanctions for non-compliance with privacy laws. However, unlike penal provisions, AMPs are not intended to be punitive, but rather aimed at ensuring statutory compliance. In this vein, since Bill 64 was originally proposed, its language was amended to allow organizations that would otherwise potentially be subject to an AMP, to avoid the AMP by entering into a compliance undertaking with the CAI to take the necessary measures to remedy the contravention or mitigate its consequences.[28] The CAI will establish and publish a general framework that will elaborate upon the mechanisms of the AMP regime, including the criteria to be used in determining the amount of a penalty. Perhaps in response to criticism over the one-size-fits-all approach of the originally proposed enforcement regime, the framework criteria have been amended to take into account the capacity of the organization in default to pay, particularly in light of its assets, sales, or income.

Organizations that violate the Act will now also face the **risk of being fined from $15,000 to the greater of $25,000,000 or 4% of their worldwide turnover** for the preceding fiscal year. These amounts are doubled for subsequent offences. In addition to many of the scenarios that may give rise to an AMP, scenarios under which an organization is deemed to have committed an offence and would therefore be subject to a fine include

where the organization: (i) 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, (ii) impedes the progress of an inquiry or inspection of the CAI, (iii) contravenes whistle-blower protections, (iv) refuses or neglects to comply, within the specified time, with a CAI demand to produce information, or (v) fails to comply with an order of the CAI.[29]

Penal provisions are generally reserved for egregious or repeat offenders and such an organization could technically be subject to both an AMP and a fine under the penal regime. The reformed penal provisions are a far cry from the existing maximum penalty of $10,000 for an initial offence under the Act, or $50,000 for communicating information outside of Québec in contravention of the Act, and instead resemble the penalties imposed under GDPR.

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 maximum penalty in force will increase ten-fold from $10,000 for most initial offences under the existing regime to $100,000 under the new regime. The latter maximum amount was doubled during parliamentary review of Bill 64, which indicates that the legislature is intent on ensuring that privacy compliance is taken seriously at the highest levels of organizations.

Lastly, the Act will now grant 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* ("**Civil Code**"). When such an infringement is intentional or results from gross negligence, the victim would be entitled to punitive damages of at least $1,000. During parliamentary review of Bill 64, the language associated with this private right of action was revised, adding doubt as to whether this right of action extends to any general infringement of a person's privacy rights under the Act or Civil Code, or only to instances where the infringement is intentional or results from gross negligence. We will have to wait to see the extent to which courts will be willing to accommodate such a right. Regardless, such a private right of action will undoubtedly contribute to an increase of privacy-related class actions.[30]

5. Conclusion

Revision of Québec's privacy legislation has been anticipated for a long time. This modernization will arguably make Québec's privacy regime the strictest on this side of the Atlantic. In addition to better aligning the province's legislation with other Canadian legislation (e.g., PIPEDA), the amendments make Québec's private-sector privacy laws 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 transmissions of personal information between Québec and Europe. Although PIPEDA has "adequacy" status for the transmission of data governed by GDPR, the same does not apply to Québec. The new requirements may help Québec obtain "adequacy" status, allowing for the unfettered transmission of data between Québec and Europe, even if some key points are still missing, such as an explicit exception to consent regarding the collection, use, or communication of personal information required for managing an employment relationship.

In addition, enforcement of the reformed Act will likely be difficult at the outset, including a potential deluge of data breach notifications, as has occurred elsewhere in Canada and Europe. Accordingly, expect to see the Québec privacy watchdog increase in size and budget over the coming years.

In light of the forthcoming effects of the reformed legislation, organizations operating in Québec should consider the following:

- Appoint a Privacy Officer;
- Implement or revise their privacy framework, including privacy policies and practices;
- Review their upstream and downstream contractual obligations regarding the protection of personal information;
- Evaluate existing physical, organizational, and technological privacy safeguards;
- Conduct a data audit/mapping to determine cases where appropriate consent could be missing;
- Implement a consent management system;
- Implement or revise retention and confidentiality incident response policies and procedures; and
- Implement or revise access request and complaint handling procedures.

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.

[1] Section 3.1 (new) of the Act.
[2] Sections 3.5 to 3.8 (new) of the Act.
[3] Section 81.3 (new) of the Act.
[4] Section 18.4 (new) of the Act.
[5] Sections 21 (replaced) to 21.0.2 (new) of the Act.
[6] Sections 3.2 (new) of the Act.
[7] Section 8 (amended) of the Act.
[8] Sections 8.1 to 8.3 (new) of the Act.
[9] Sections 3.3 and 3.4 (new) of the Act.
[10] Section 9.1 (new) of the Act.

[11] Sections 8.3 (new) and 14 (amended) of the Act.
[12] Article 4(11) of GDPR.
[13] Section 12 (replaced) of the Act.
[14] Sections 18 (amended) and 22 (deleted) of the Act.
[15] Section 12 (replaced) of the Act.
[16] Sections 4.1 (new) and 14 (amended) of the Act.
[17] Section 11 (amended) of the Act.
[18] Section 12.1 (new) of the Act.
[19] Section 17 (amended) of the Act.
[20] Section 1 (amended) of the Act.
[21] Section 18.3 (new) of the Act.
[22] Section 28.1 (new) of the Act.
[23] Section 23 (replaced) of the Act.
[24] Section 27 (amended) of the Act.
[25] Section 81 (amended) of the Act.
[26] Section 81.1 (new) of the Act.
[27] Sections 90.1 to 90.17 (new) of the Act.
[28] Section 90.1 (new) of the Act.
[29] Section 91 to 93 (replaced and new) of the Act.
[30] Section 93.1 (new) of the Act.

by Rish Handa.

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.