mcmillan

BILL 64: A CHECKLIST TO HELP BUSINESSES COMPLY WITH MODERN PRIVACY REQUIREMENTS IN QUÉBEC

Posted on December 1, 2021

Categories: Insights, Publications

On September 22, 2021, Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (the "***Privacy Modernization Act***" or the "***Amended Act***") received royal assent.[1] The Privacy Modernization Act updates Québec's *Act respecting the protection of personal information in the private sector* (the "***Act***")[2] to fit the modern era of data protection and keep pace with international privacy developments (the "**amendments**").

Notably, the amendments provide for enhanced enforcement mechanisms, including administrative monetary penalties, a private right of action for individuals, and fines of up to $25 million for organizations that fail to comply with the *Act*.

While we have already provided a substantive bulletin on how the *Privacy Modernization Act* will transform the *Act*, this bulletin provides a checklist of key action items as the legislation comes into force over the next three years.

Does the *Act* Apply to My Organization?

Québec's privacy regulator, the Commission d'accès à l'information (the "**CAI**"), has taken an expansive view of how the *Act* applies. If an organization collects, uses or discloses personal information ("**PI**") of individuals **located within Québec**, the *Act* likely applies to the organization's handling of PI, even if the organization does not have an office, facilities or installations in Québec.[3] The Act will also apply concurrently with the *Personal Information Protection and Electronic Documents Act* ("***PIPEDA***")[4] for federally-regulated organizations, such as banks, railways or airlines, that would normally be subject to *PIPEDA*.[5]

Accordingly, any organization that handles PI about individuals in Québec should assess how these amendments will impact its operations and start implementing necessary changes as soon as possible.

Privacy Compliance Checklist

(click here for a one-page version of the checklist)

By September 22, 2022

¨ Appoint a Privacy Officer (if you do not already have one).

- Appoint an individual that will be responsible for ensuring that the organization complies with the obligations imposed by the *Amended Act*. By default, this responsibility falls on the person with the highest authority in the company (likely the Chief Executive Officer), but can be delegated, in whole or in part, to any other person (internal or external).
- If applicable, have the person with the highest authority in the company delegate their role in writing to the appointed Privacy Officer.
- Post the title and contact information of the appointed Privacy Officer on your website.

¨ Review and update your data breach response plan.

- As soon as you have reason to believe that a Confidentiality Incident (e.g. data breach) involving PI in your custody has occurred, take reasonable measures to reduce any risk of harm and to prevent similar incidents.
    - Under the *Amended Act*, a Confidentiality Incident is defined as access to, use, or communication of PI not authorized by law, as well as the loss or any infringement of the protection of such information.
- Notify the CAI and any affected individuals if there is risk of serious injury to those individuals.[6]
- The assessment of risk must take into account certain factors.[7] The forthcoming regulations will likely provide details regarding the form of the notice. The CAI may also publish helpful guidance in this regard.[8]

¨ Familiarize yourself with obligations when disclosing PI as part of a commercial transaction.

- Where the disclosure of PI is necessary in order to carry out a commercial transaction (e.g. merger, asset sale or financing), you may disclose such PI to another party involved in the transaction without the concerned person's consent.
- If your company transfers PI to facilitate such a transaction, enter into an agreement that meets certain requirements designed to protect the PI transferred. These requirements are in line with privacy legislation throughout Canada.

By September 22, 2023

¨ Develop your privacy framework / update your online privacy policy.

- Develop and implement a privacy framework outlining your policies and practices with respect to the

organization's use and protection of PI.[9] This framework should include a data breach response plan, retention schedules, the roles and responsibilities of the members of the organization's personnel throughout the life cycle of PI and procedures for access requests and handling complaints.
- Publish clear, simple, and detailed information about these policies and practices on your website.[10]
- If you collect PI through technological means, provide a confidentiality policy that is written in clear and simple language on your website.[11]

¨ Develop a Privacy Impact Assessment system.

- Carry out Privacy Impact Assessments ("**PIAs**") for each project involving the acquisition, development, or redesign of an information system or electronic service delivery involving PI.[12]
    - Consult your Privacy Officer at the outset of the PIA. Your Privacy Officer may suggest adding protection measures for PI that are relevant in the context of the project.[13]
    - Ensure that the project allows for any computerized PI to be transferred to the individual concerned in a structured, commonly used format (this will also be necessary to comply with the data portability requirement coming into force in 2024).[14]
- Conduct a PIA before communicating PI outside of Québec. The PIA must take into account certain factors, including the sensitivity of the information, the purposes for which the PI will be used and the legal framework applicable in the foreign jurisdiction to which the information will be communicated.[15]
    - If you communicate PI outside Québec, develop and implement a written agreement that considers the results of the PIA and, if applicable, terms agreed on to mitigate risks identified in the PIA.
- Review the CAI's published guidance on PIAs[16] to make sure your PIA system is consistent with the regulator's expectations.
- Consider hiring additional privacy compliance professionals to assist you in conducting PIAs and meeting your obligations under the *Amended Act*, especially if you are a large organization. Depending on the number of service providers or technological projects you use in the ordinary course of business, this requirement may be quite onerous.

¨ Review/implement contracts with third party service providers.

- The *Amended Act* does not require consent where information is communicated to a third party (i.e. service provider), to the extent the information is necessary to carry out a mandate or perform a contract of enterprise or for services.[17]
- If you communicate PI to service providers, you must have a written contract that includes: (i) a list of the measures the service provider must take to protect the PI communicated, (ii) a requirement for the

service provider to only use PI for the purposes of performing the contract, (iii) an obligation for the service provider not to keep the information after the expiry of the contract, (iv) a requirement for the service provider to immediately notify the Privacy Officer of any actual or attempted violation of the confidentiality of the PI, and the Privacy Officer's right to audit compliance with protective measures.[18]
- If the third party/service provider is handling PI outside Québec, a PIA must be conducted (see section above regarding PIAs).[19]

¨ Assess your physical, organizational, and technological safeguards.

- While the requirements for safeguards have not changed,[20] penalties for non-compliance will significantly increase under the *Privacy Modernization Act*. The hefty penalties, combined with the increase in cyber-crime resulting from the pandemic, justifies a re-assessment of safeguards in place to ensure that they are sufficient to adequately protect PI.

¨ Review your insurance coverage.

- Risk of liability is increased due to the fines, penalties and private right of action that are prescribed within the *Amended Act*.
- Renegotiate your cyber-risk insurance coverage to ensure that your organization is adequately protected.

¨ Familiarize yourself with new consent requirements and exceptions.

- Obtain consent that is "clear, free, and informed."[21] While the *Act* currently requires consent that is "manifest, free, and enlightened",[22] this change indicates a shift towards allowing implied consent in some circumstances.[23]
- Obtain express consent when sensitive information is involved.[24] This includes information that has a high level of reasonable expectation of privacy and includes medical, biometric, or other intimate information.[25]
- Familiarize yourself with new consent exceptions, particularly when using PI for purposes beyond those for which it was originally collected.[26] Under the *Amended Act*, consent is not required where the new use is:

    i. For purposes consistent with those for which it was collected;
    ii. clearly for the benefit of the person concerned;
    iii. necessary for the prevention 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, subject to the PI being de-identified.[27]

- Obtain the consent of a person with parental authority when collecting, using, or disclosing information concerning a minor under the age of 14, unless the information is clearly in the minor's benefit.[28]

¨ Update your consent forms / implement a consent management system.

- Upon collecting information from an individual, inform them of:

  i. The purposes for which the information is collected;
  ii. the means by which it is collected;
  iii. their rights of access and rectification, and
  iv. their right to withdraw consent.[29]

- If applicable, inform individuals of the name of the third person for whom the information is being collected. Where the information is transferred to third parties, inform the individual of the names or categories of third persons, and the possibility that the information could be communicated outside Québec.
- Any request for consent must be made in clear and simple terms and requested for each specific purpose for consent to be valid. If the request for consent is made in writing, present it independently from any other information disclosed to the person.
- Consent gathered in contravention of the *Amended Act* will be null and void.[30] As such, consider implementing a consent management system to track what consent has been provided and where additional consent is required.

¨ Know your transparency obligations (including for tracking and profiling).

- If an individual requests so, inform them of the PI collected from them, the categories of persons who have access to their information within the enterprise, the length of time the information will be kept, and the contact information of the person in charge of protecting PI.[31]
- If you collect information using technology that allows an individual to be identified, located, or profiled, inform the individual of the use of this technology and the means available to activate the technology (the technology should be deactivated by default).[32]
- In certain circumstances and where applicable, notify individuals that you use automated decision-making (see "prepare notices for automated decision making" below).

¨ Implement privacy-by-default.

- Set public-facing technological products or services to the highest privacy parameters by default.[33] Cookies are excluded from this requirement.[34]

¨ Review and update your retention schedules.

- Where PI is used to make a decision about an individual, retain that PI for at least one (1) year. This is in line with requirements under *PIPEDA* and other privacy legislation in Canada.[35]
- Where the PI is no longer necessary for its purposes, and subject to any preservation period provided for by legislation, destroy the PI or anonymize it in order to use it for a serious and legitimate purpose.[36]

¨ Review your data anonymization process (if applicable).

- Anonymize data in order to use it for purposes for which it was not originally collected, without requiring additional consent. Note that true data anonymization is very difficult to achieve.
- Under the *Amended Act*, PI is deemed "anonymized" when it is, at all times, reasonable to expect that it irreversibly no longer allows the person to be identified, directly or indirectly.[37]
- Anonymize data according to generally accepted best practices. The forthcoming regulations will further specify what these best practices entail.[38]

¨ Prepare notices and explanatory language for automated decision-making.

- Notify the person concerned if you make a decision exclusively based on automated decision-making using PI collected from them.[39]
- Upon request, inform the individual of (i) the PI used to render the decision, (ii) the reasons and principal factors and parameters that led to the decision, and (iii) the right of the person concerned to have relevant information corrected.[40]
- Assess your use of automated decision-making, and prepare to explain decision-making in clear and simple language.

By September 22, 2024

¨ Ensure your data management systems allow data to be extracted and transferred.

- The *Amended Act* provides individuals with the right to request that their information be communicated or transferred to them, or a third party organization, in a structured and commonly used format.
- This does not apply to information that has been generated or inferred from an individual's PI (e.g. statistics about the individual) and will not apply in circumstances that raise serious practical difficulties.
- Meeting this obligation could take significant lead-time, or require an overhaul of data processing systems, depending on, for example, the format of the data, and the degree to which individuals' PI is

mixed with proprietary information or information of other individuals.

If you have any questions about how to best prepare for these changes, the lawyers in our Privacy and Cybersecurity Group would be happy to assist you.

(click here for a one-page version of the checklist)

[1] *An Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021, c 25.
[2] *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1. [**Act**]
[3] PIPEDA Report of Findings #2021-001, February 2, 2021, para 34.
[4] *D'Allaire c. Transport Robert (Québec) 1973 ltée*, 2020 QCCAI 152.
[5] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.
[6] *Act* (as amended), section 3.5.
[7] *Act* (as amended), section 3.7.
[8] *Act* (as amended), section 3.5; the CAI has also developed a dedicated page for guidance on the Privacy Modernization Act: see online.
[9] *Act* (as amended), section 3.2.
[10] *Act* (as amended), section 3.2.
[11] *Act* (as amended), section 8.2.
[12] *Act* (as amended), section 3.3.
[13] *Act* (as amended), section 3.4.
[14] *Act* (as amended), section 3.3.
[15] *Act* (as amended), section 17.
[16] Commission d'accès à l'information du Québec, *Guide d'accompagnement Réaliser une évaluation des facteurs relatifs à la vie privée*, March 2021, available online.
[17] *Act* (as amended), section 18.3.
[18] *Act* (as amended), section 18.3.
[19] *Act* (as amended), section 17.
[20] *Act*, section 10.
[21] *Act* (as amended), section 14.
[22] *Act*, section 14.
[23] See, for example, section 8.3 of the Act (as amended), which provides that where an individual provides their information after receiving the required notices, they consent to the use and communication of their information for the purposes provided.
[24] *Act* (as amended), section 12.
[25] *Act* (as amended), section 12.

[26] *Act* (as amended), section 12.
[27] *Act* (as amended), section 12.
[28] *Act* (as amended), section 4.1.
[29] *Act* (as amended), section 8.
[30] *Act* (as amended), section 14.
[31] *Act* (as amended), section 8.
[32] *Act* (as amended), section 8.1.
[33] *Act* (as amended), section 9.1.
[34] *Act* (as amended), section 9.1.
[35] Act (as amended), section 11.
[36] *Act* (as amended), section 23.
[37] *Act* (as amended), section 23.
[38] *Act* (as amended), section 23.
[39] *Act* (as amended), section 12.1.
[40] *Act* (as amended), section 12.1.

by Robbie Grant and Marie-Eve Jean

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.