Client Advisory: Noteworthy Changes to Québec's Private Sector Privacy Law and Other Amendments

Olalekan (Wole) Akinremi, Imtiaz Karamat, Sharan Johal, and Victoria Di Felice January 24, 2023

Introduction

Certain amendments to Québec's *Act respecting the protection of personal information in the private sector* (the "Québec Act") and the *Act to establish a legal framework for information technology* (the "Québec IT Act") introduced by *The Privacy Legislation Modernization Act* ("Law 25"),[1] took effect on September 22, 2022. The purpose of this advisory is to provide an overview of the requirements under the Québec Act and the Québec IT Act that came into effect on September 22, 2022.

We will also refer to the requirements of the Regulation respecting confidentiality incidents (the "Regulation"). The Regulation came into force on December 29, 2022,[2] and sets out additional notification and record-keeping requirements with respect to confidentiality incidents.

The Québec Act, the Québec IT Act, and the Regulation[3] will apply to any private sector organization that: (i) is established in Québec; or (ii) if established outside of Québec, operates in Québec.

This advisory also compares the provisions under the Regulation and the provisions in Law 25 that came into effect on September 22, 2022, with the analogous provisions under the federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and the *Breach of Security Safeguards Regulations* ("PIPEDA Regulation").

At the end of this advisory, checklists have been provided to assist organizations with their compliance with the new requirements under the Québec Act, the Québec IT Act, and the Regulation.

Overview

This advisory is divided into the following parts.

1. Mandatory Breach Reporting and Record-Keeping Requirements
    A. Confidentiality Incidents
    B. Mitigation of Risk
    C. Notification of Confidentiality Incidents
    D. Content of Notices
    E. Registry of Confidentiality Incidents
2. The Requirement to Designate a Person in Charge of Protection of Personal Information
    A. Designation
    B. Duties

[1] Since Bill 64 received formal assent on September 22, 2021, it became *The Privacy Legislation Modernization Act* – also known as Law 25.
[2] With respect to political parties, independent Members, and independent candidates, the Regulation takes effect on September 22, 2023.
[3] Please note that the Québec IT Act and the Regulation also applies to public sector institutions.

This advisory is not intended to be a complete statement of the law and does not constitute legal advice. As this advisory is for information purposes only, no person should act or rely upon the information contained in this advisory without seeking legal advice.

---

1. Mandatory Breach Reporting and Record-Keeping

A. *Confidentiality Incidents*

Sections 3.5 to 3.8 of the Québec Act outline several requirements that organizations must comply with in the event that they suffer a "confidentiality incident".

Section 3.6 of the Québec Act defines a "**confidentiality incident**" as:

(1) access not authorized by law to personal information;

(2) use not authorized by law of personal information;

(3) disclosure not authorized by law of personal information; or

(4) loss of personal information or any other breach in the protection of such information.

By comparison, PIPEDA outlines certain steps organizations must take in the event of a "breach of security safeguards". Section 2(1) of PIPEDA defines a "**breach of security safeguards**" as "a loss, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from failure to establish those safeguards."

While the definition of a "confidentiality incident" covers similar circumstances as the definition of "breach of security safeguards", a "confidentiality incident" also includes "any other breach in the protection of [personal] information." As a result, under the Québec Act, organizations may be required to monitor a broader spectrum of cybersecurity risks to identify confidentiality incidents that trigger reporting and record keeping obligations.

B. *Mitigation of Risk*

Section 3.5 of the Québec Act requires an organization that has cause to believe that a confidentiality incident has occurred to take reasonable measures to reduce the risk of injury and to prevent future incidents of the same nature from occurring. PIPEDA does not impose a corresponding obligation on organizations to take steps to prevent future incidents from occurring.

C. *Notification of Confidentiality Incidents*

Section 3.5 of the Québec Act also requires that if a confidentiality incident poses a "risk of serious injury", the organization must promptly notify the Commission d'accès à l'information

(the "CAI") and any person whose personal information is impacted by the confidentiality incident. PIPEDA requires notification as soon as possible to the Office of the Privacy Commissioner (the "OPC") if a breach of security measures presents a "real risk of significant harm". It is unclear whether there is a material difference between a "risk of serious injury" and a "real risk of significant harm". However, organizations should be mindful of the possibility that the standard in Québec may be interpreted in a manner that is more stringent than the standard in PIPEDA.

Section 3.7 of the Québec Act does not provide a clear definition of a "risk of serious injury", but it outlines the factors that organizations must consider in assessing the risk of injury to a person whose personal information is impacted by a confidentiality incident. The "**risk of serious injury**" factors to be considered are:

(1) the sensitivity of the information;

(2) the anticipated consequences of its use; and

(3) the likelihood that such information will be used for injurious purposes.

In contrast, PIPEDA provides a definition of "significant harm". Under Section 10.1(7) of PIPEDA, "**significant harm**" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

Furthermore, Section 10.1(8) of PIPEDA sets out the following factors to be considered when determining whether a breach of security safeguards creates a "**real risk of significant harm**":

(1) the sensitivity of the personal information involved in the breach;

(2) the probability that the personal information has been, is being or will be misused; and

(3) any other prescribed factor.

D. *Content of Notices*

Section 3 of the Regulation specifies the content that must be included in the notice provided to the CAI.[4]

When providing written notice to the CAI, the following information **must be provided**:

(1) the name of the organization and if applicable, its Québec business number;

(2) the name and contact information of the person to be contacted in that organization with regard to the incident;

(3) a description of the personal information affected by the incident or, if that information is not known, the reasons why it is impossible to provide such a description;

(4) a description of the circumstances and, if known, the cause of the incident;

(5) the date or time period when the incident occurred or, if unknown, the approximate time period;

(6) the date or time period when the organization became aware of the incident;

[4] As stated earlier, under Section 3.5 of the Québec Act, notice is required when the confidentiality incident involves a risk of serious injury.

(7) the number of individuals affected, including the number of affected Québec residents or, if that is not known, the approximate numbers;

(8) the steps the organization has taken or intends to take to notify the individuals affected, as well as the date when affected individuals were notified, or the expected time limit for the notification;

(9) a description of the elements that led the body to conclude that there is a risk of serious injury to the persons concerned (i.e., the sensitivity of personal information, any possible ill-intentioned uses of such information, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes);

(10) the steps the organization has taken or intends to take to reduce the risk of injury and prevent new incidents of the same nature and the date or time period when the steps were taken or will be taken; and

(11) if applicable, an indication that a privacy commissioner outside of Québec has been notified of the incident.

The requirements in Section 3 of the Regulation are very similar to the requirements in Section 2 of the PIPEDA Regulation.[5]

Section 4 of the Regulation requires organizations to promptly provide the CAI with the information prescribed in Section 3 of the Regulation that the organization was unable to provide in its initial notice.[6] This obligation to notify the CAI contrasts with the discretionary obligation to notify the OPC of any new information related to the breach.[7]

Section 5 of the Regulation specifies the content that must be included in the notices provided directly to affected individuals.[8] The notification obligations under Section 5 of the Regulation are very similar to the requirements under Section 3 of the PIPEDA Regulations.

Under Section 5 of the Regulation, when providing written notice to affected individuals, the following information **must be provided**:

(1) a description of the personal information affected by the confidentiality incident or, if that information is not known, the reasons why it is impossible to provide such a description;

(2) a description of the circumstances of the incident;

(3) the date or time period when the incident occurred or, if unknown, the approximate time period;

(4) the steps the organization has taken or intends to take to reduce the risk of injury;

(5) the steps that can be taken by the individual to reduce the risk of injury or to mitigate the injury resulting from the incident; and

(6) the organization's contact information.

[5] Section 2 of the PIPEDA Regulation sets out the content, form and manner of the notice that must be sent to the OPC.
[6] The obligation to provide further notice to the CAI is triggered once the organization becomes aware of new information.
[7] Under Section 2.2 of the PIPEDA Regulation, organizations *may* submit any new information related to the breach to the OPC that the organization becomes aware of after having made the initial report to the OPC.
[8] As stated earlier, notice is required when the confidentiality incident involves a risk of serious injury.

Section 6 of the Regulation provides an exception to the direct notification requirement outlined in Section 5 of the Regulation.[9] Notice to affected individuals is to be provided by way of a public notice (using any method that could be reasonably expected to reach the individual affected) in any of the following circumstances:

(1) when sending such notice is likely to cause increased injury to the individual affected;

(2) when sending such notice is likely to cause undue hardship for the organization; or

(3) when the organization does not have the contact information for the individual affected.

Section 6 of the Regulation also provides that if there is a need to act rapidly to reduce the risk of a serious injury or to mitigate any such injury, the organization can also provide notice by way of a public notice. However, the organization will also be required to directly notify the individuals affected, unless one of the circumstances listed in Section 6 of the Regulation applies.

Lastly, Section 3.5 of the Québec Act provides that an organization is not required to notify an individual if doing so "could hamper an investigation conducted by a person or body responsible by law for the prevention, detection or repression of crime or statutory offences."

E. *Registry of Confidentiality Incidents*

Section 3.8 of the Québec Act requires an organization to maintain a register of all confidentiality incidents, a copy of which must be sent to the CAI upon request.

Section 7 of the Regulation specifies that the register **must contain the following information**:

(1) a description of the personal information affected by the incident or, if that information is not known, the reasons why it is impossible to provide such a description;

(2) a description of the circumstances of the incident;

(3) the date or time period when the incident occurred or, if that is not known, the approximate time period;

(4) the date or time period when the organization became aware of the incident;

(5) the number of persons affected by the incident or, if that is not known, the approximate number;

(6) a description of the elements that led the organization to conclude whether or not there is a risk of serious injury to the individuals affected;

(7) if the incident presents a risk of serious injury, the dates notices were sent to the CAI and the individuals affected, as well as an indication of whether the organization issued public notices and, if applicable, its reasons for doing so; and

(8) a description of the measures the organization has taken after the incident occurred in order to reduce the risks of injury.

Section 8 of the Regulation requires that the information in the register must be kept up to date, and must be retained for **a minimum of 5 years** after the date or time period when the organization became aware of the confidentiality incident. By contrast, the PIPEDA Regulation **does not expressly require** the record of the breach of security safeguard to be

[9] Section 6 of the Regulation is analogous to Section 5 of the PIPEDA Regulation.

kept up to date, and only requires the record of the breach to be kept for 24 months after the day the organization determines the breach had occurred.

If your organization conducts business in multiple provinces that include Québec, it may be prudent to maintain a register of the confidentiality incidents involving Québec and a separate register for breaches of security safeguards involving personal information occurring across Canada (including Québec). Maintaining a separate register for Québec may decrease the likelihood of inadvertent disclosure to the CAI regarding breaches of security safeguards that occurred outside of Québec.

2. Requirement to Designate a Person in Charge of Protection of Personal Information

A. *Designation*

Section 3.1 of the Québec Act requires organizations to designate a person in charge of the protection of personal information and for ensuring compliance with the Québec Act. Organizations must publish this person's title and contact information on their website (and if the organization does not have a website, by any other appropriate means).

This responsibility defaults to the "person exercising the highest authority" within the organization. However, this person may delegate, in writing, all or part of "the function of the person in charge of the protection of personal information" to "any person".

B. *Duties*

Under Sections 3.2 and 3.3 of the Québec Act, **the designated individual must, at a minimum**:

(1) establish governance policies and practices regarding the protection of personal information; and

(2) oversee any privacy impact assessment conducted for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, disclosure, keeping, or destruction of personal information.

3. Exceptions to the Consent Requirement

Law 25 introduced new exceptions to the requirement to obtain consent for certain uses or disclosures of personal information. The majority of these exceptions come into force on September 22, 2023. However, two exceptions, namely: (i) the disclosure of personal information for concluding a commercial transaction; and (ii) the disclosure of personal information for study, research, or statistical purposes, each came into force on September 22, 2022.[10]

A. *Disclosure of Personal Information for Concluding a Commercial Transaction*

Section 18.4 of the Québec Act defines a "**commercial transaction**" as "the alienation or leasing of all or part of an enterprise or of its assets, a modification of its legal structure by merger or otherwise, the obtaining of a loan or any other form of financing by the organization or of a security taken to guarantee any of its obligations." Section 18.4 of

[10] These two exceptions are similar to the research exception (Section 7(3)(f)), and the business transaction exception (Section 7.2(1)) found in PIPEDA.

the Québec Act also provides that where the disclosure of personal information is necessary for concluding a commercial transaction, personal information may be disclosed to a third party involved in the transaction without the consent of the individual.

However, pursuant to Section 18.4 of the Québec Act, the organization disclosing personal information to the third party **must first enter into an agreement** with such party that specifies that the third party undertakes:

(1) to use the information only for the purpose of completing the commercial transaction;

(2) not to disclose the information without the consent of the individual concerned, unless authorized to do by the Québec Act;

(3) to take the measures required to protect the confidentiality of the information; and

(4) to destroy the information if the commercial transaction is not completed or if the use of personal information is no longer necessary for concluding the commercial transaction.

If the third party wishes to continue to use or disclose the personal information after the commercial transaction has been completed, the third party may only use or disclose such information in accordance with the Québec Act. Also, within a reasonable time after the commercial transaction is completed, the third party must notify the individual (that the personal information is about) that it now holds their personal information as a result of the completed transaction.

B. *Disclosure of Personal Information for Study, Research, or Statistical Purposes*

Under Section 21 of the Québec Act, an organization may disclose, without the consent of the individual, personal information about the individual to a third party wishing to use the information **for study, research or the production of statistics**. Section 21 of the Québec Act also provides that the personal information may only be disclosed if a privacy impact assessment conducted by the organization concludes that:

(1) the personal information is needed to achieve the objective of the study or research or the production of statistics;

(2) it is unreasonable to require the third party to obtain consent;

(3) the objective of the study or research or the production of statistics outweighs, having regard to the public interest, the impact of disclosing and using such information on the individual's privacy;

(4) the personal information is used in a manner that ensures its confidentiality; and

(5) only necessary information is disclosed.

Obligations for Requesting Third Parties

Section 21.0.1 of the Québec Act states that the third party wishing to use the personal information for study, research or the production of statistics **must make the request in writing** and provide the disclosing organization with:

(1) a detailed presentation of the research activities,

(2) the grounds supporting the fulfilment of the criteria required to be established by the PIA required under Section 21 of the Québec Act;

(3) a list of all other parties to whom a similar request is being made for the purposes of the same study, research or production of statistics;

(4) if applicable, a description of the technologies that will be used to process the information; and

(5) if applicable, the documented decision of a research ethics committee relating to the study, research or the production of statistics.

Mandatory Agreement Provisions

Section 21.0.2 of the Québec Act requires the parties to the disclosure of personal information (for study, research purposes or the production of statistics) to **enter into an agreement** that stipulates that the information:

(1) may be made accessible only to persons who need to know it to exercise their functions and who have signed a confidentiality agreement;

(2) may not be used for purposes other than those specified in the detailed presentation of research activities;

(3) may not be matched with any other information file that has not been provided for in the detailed presentation of research activities; and

(4) may not be disclosed, published or otherwise distributed in a form allowing any individual (whose personal information had been disclosed) to be identified.

The agreement must also:

(1) specify the information that must be provided to the individuals whose personal information had been disclosed if their personal information is used to contact them to participate in the study or research;

(2) provide measures for ensuring the protection of the personal information;

(3) determine a preservation period for the personal information;

(4) set out the obligation to notify the person who communicates the personal information of its destruction; and

(5) provide that the person who communicates the personal information and the CAI must be informed without delay:

(i) of non-compliance with any condition set out in the agreement;

(ii) of any failure to comply with the protection measures provided for in the agreement; and

(iii) of any event that could breach the confidentiality of the information.

Additionally, Section 21.0.2 of the Québec Act requires the signed agreement to be sent to the CAI and provides that the agreement will be effective 30 days after it is received by the CAI.

4. Verification or Confirmation of Identity by Biometric Means

Previously, under Section 44 of the Québec IT Act, an individual's identity could not be verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded, except with the express consent of the individual. However,

as of September 22, 2022, in addition to the aforementioned express consent requirement, Section 44 of the Québec IT Act now requires organizations **to disclose to the CAI** (in advance) their use of any process that allows biometric characteristics or measurements to be recorded for the purpose of verifying or confirming an individual's identity. Additionally, only the **minimum number of characteristics or measurements** needed to link the individual to an act and only such characteristics or measurements as may not be recorded without the individual's knowledge may then be used for identification purposes.

5. Biometric Database Registration

Prior to September 22, 2022, Section 45 of the Québec IT Act required organizations to notify the CAI beforehand (with no timeline specified) of the creation of a database of biometric characteristics and measurements. Additionally, organizations also had to disclose to the CAI the existence of the database (whether or not it is in service). However, as of September 22, 2022, organizations **must promptly, and no later than 60 days** before the database of biometric characteristics and measurements is brought into service, disclose to the CAI the creation of a database of biometric characteristics and measurements.

Conclusion

Your organization should, as soon as possible, begin to update (or develop) policies that are affected by the recent changes introduced by Law 25 and the Regulation. Reviewing each checklist in this advisory may assist your organization's compliance with these recent changes.

If you have further questions, please contact a member of our Technology Group.

Appendix A

Compliance Checklists

1. Mandatory Breach Reporting and Record-Keeping

The following checklist is a guide to assist organizations in ensuring compliance with the mandatory breach reporting and record-keeping requirements under the Québec Act.

Checklist for Compliance with the Mandatory Breach Reporting and Record Keeping Requirements:

☐ Has your organization developed a breach response plan that outlines the steps:

- to assess whether a confidentiality incident presents a risk of serious injury to the affected individuals? and
- that can be taken to reduce the risk of injury to individuals who are affected by a confidentiality incident?

☐ Has your organization established a process to ensure the CAI (and if applicable, other regulatory authorities) and individuals affected are promptly notified following the occurrence of a confidentiality incident?

☐ Has your organization developed template notices to the CAI and to individuals affected that meet the regulatory requirements?

☐ Has your organization established a process to provide public notice of confidentiality incidents if a direct notification to the affected individuals is not feasible?

☐ Has your organization established compliance policies to ensure a register of confidentiality incidents is appropriately maintained?

☐ Are there retention mechanisms in place to ensure that for a confidentiality incident, the register is retained for at least 5 years after your organization became aware of such incident?

2. Requirement to Designate a Person in Charge of Protection of Personal Information

The following checklist is a guide to assist organizations in ensuring compliance with the obligations under the Québec Act to designate a person in charge of protection of personal information.

Checklist for Compliance with the Requirement to Designate a Person in Charge of the Protection of Personal Information:

☐ Has your organization designated an appropriate individual to be responsible for the protection of personal information and compliance with your organization's obligations under the Québec Act?

- Is this individual familiar with their obligations?
- Has this individual delegated all or part of their responsibilities to any person? If so, is this delegation in writing?

☐ Has your organization published the designated individual's title and contact information on its website?

☐ Has your organization (with the oversight of the designated individual) established governance policies and practices regarding the protection of personal information?

3. Disclosure of Personal Information for Concluding a Commercial Transaction

The following checklist is a guide to assist organizations in ensuring compliance with the obligations under the Québec Act relating to the disclosure of personal information (without consent) to conclude a commercial transaction.

Checklist for Compliance with the Consent Exception – Disclosure of Personal Information Without Consent to Conclude a Commercial Transaction:

A. Organizations Disclosing Personal Information to a Third Party:

☐ Does your organization engage in "commercial transactions" as defined in Section 18.4 of the Québec Act?

☐ If yes, will your organization be disclosing to a third party, without consent, the personal information of Québec residents in connection with a commercial transaction?

☐ If yes, has your organization developed a template agreement regarding the handling of personal information (in connection with a commercial transaction) by a third party that meets the requirements of Section 18.4 of the Québec Act?

☐ If yes, in connection with the commercial transaction and before disclosing the personal information to the other party, did you enter into the template agreement with such third party?

B. Organizations Receiving Personal Information from a Third Party:

☐ Has your organization received personal information (of Québec residents) from a third party for the purpose of completing a commercial transaction?

☐ If yes, does your organization wish to continue to use and disclose such personal information after the commercial transaction is completed?

☐ If yes, has your organization promptly notified individuals informing them that your organization now holds personal information about them as a result of the completed transaction?

4. Disclosure of Personal Information for Study, Research, or Statistical Purposes

The following checklist is a guide to assist organizations in ensuring compliance with the obligations under the Québec Act relating to the disclosure of personal information (without consent) for study, research or statistical purposes.

Checklist for Compliance with the Disclosure of Personal Information for Study, Research or Statistical Purposes:

- ☐ Does your organization disclose personal information (of Québec residents) without consent for study, research, or statistical purposes?
- ☐ If yes, does your organization have a process in place to conduct a Privacy Impact Assessment to ensure the criteria under Section 21 of the Québec Act are met?
- ☐ If yes, has your organization developed compliance procedures to ensure that your organization has received, from the party requesting the personal information, all the information required under Section 21.0.1 of the Québec Act?
- ☐ Has your organization developed a template agreement (regarding the disclosure of personal information without consent for study, research, or statistical purposes) that meets the requirements of Section 21.0.2 of the Québec Act?
- ☐ Has your organization developed compliance procedures to ensure that the CAI has received a copy of the agreement entered into between your organization and the party requesting the personal information for study, research, or statistical purposes?
- ☐ Has the agreement been entered into on the basis that it will only become effective thirty days after the agreement is received by the CAI?

5. Verification or Confirmation of Identity by Biometric Means

The following checklist is a guide to assist organizations in ensuring compliance with the obligations under the Québec IT Act relating to verification or confirmation of an individual's identity by biometric means.

Checklist for Compliance with the Notification and Consent Requirements regarding the Verification or Confirmation of Identity by Biometric Means:

☐ Does your organization have a process to verify or confirm an individual's identity that allows biometric characteristics or measurements to be recorded?

☐ If yes:

- Has your organization established compliance procedures to ensure that the individual's express consent has been obtained?
- Has your organization established compliance procedures to ensure that the CAI is notified in advance of your organization's verification or confirmation process?
- Are there mechanisms established to ensure that for identification purposes, only the minimum number of characteristics or measurements needed to link the individual to an act are used?

6. Biometric Database Registration

The following checklist is a guide to assist organizations in ensuring compliance with the obligations under the Québec IT Act relating to the creation of a database of biometric characteristics and measurements.

Checklist for Compliance with the Notification Requirement for Biometric Databases:

☐ Has your organization developed compliance procedures to ensure that the CAI is notified no later than 60 days before the database of biometric characteristics and measurements is brought into service?