LANGLOIS

AVOCATS - LAWYERS

| | |
|---|---|
| **Title:** | **Privacy protection in Quebec: an overview of amendments to the law governing the private sector** |
| **Written by:** | **Jean-François De Rico**<br>**Lawyer, Partner** |
| | **Caroline Deschênes**<br>**Lawyer, Partner** |
| | **Pascal Archambault**<br>**Lawyer** |
| | **Justine Brien**<br>**Lawyer** |

## I. Modernizing privacy legislation

On June 12, the Quebec government introduced bill 164, *An Act to modernize legislative provisions as regards the protection of personal information* ("**the Bill**" or "**Bill 64**"), first announced nearly a year ago. Once adopted, the Bill will result in significant changes to various laws in order to modernize the regulatory framework for the protection of personal data in Quebec.

The modernization process will target private and public sector institutions as well as political parties, and will require compliance efforts by all these organizations. Indeed, the nature of the new requirements and the hefty penalties for violations mean that privacy protection can no longer be ignored with impunity.

Among other things, the Bill proposes granting new rights to individuals regarding data portability, the right to be forgotten and the right to de-indexation. In order to implement and uphold these rights, many companies will have to modify their business processes or adopt new ones.

Our team can assist with this exercise by analyzing your existing processes, identifying gaps and formulating implementation recommendations to comply with the amended law.

We begin this series of publications about the Bill with an overview of the key amendments to the *Act Respecting the Protection of Personal Information in the Private Sector* ("**PPIPS**" or the "**Act**"), which applies to any business operating in the province.

### A. Scope

The scope of the Act will remain essentially unchanged as far as businesses are concerned. However, the Bill states that:

- the personal data concerned includes personal data collected by the company, even in instances where it is stored by third party.[1]

- information relating to job title function (name, title, business address) will no longer be subject to the PPIPA;[2] this puts an end to the divided case law from the Commission d'accès à l'information (CAI) regarding the characterization of business contact information as personal information.

### B. Responsibility for personal data protection

The Bill explicitly introduces the principle of accountability by the company collecting the data,[3] which is one of the basic principles of privacy protection.

Most significantly for businesses, the responsibility for the protection of personal information, or role of "Chief Privacy Officer", will now rest with the highest ranking officer of the company. This person will now be responsible for the implementation of, and compliance with the provisions of the Act.[4] Contact details for this person or the person to whom the role is delegated will have to be published on the company's website or, in the absence of a website, made available through other means.

### C. Governance: adoption of policies and practices

Bill 64 proposes that all companies be required to adopt governance policies and practices to ensure that personal data is protected. These policies and practices should provide a framework for the following aspects, among others:

- data retention and destruction;

- staff member roles and responsibilities;

- a complaints process.[5]

These policies must be approved by the Chief Privacy Officer[6] and made publicly available on the company's website.[7] Any company collecting personal information through electronic means must communicate its privacy policy and publish it on its website.[8]

Within the governance component, the Bill also establishes a requirement for the organization to conduct a risk assessment for any project involving the collection or use of personal information. As with any obligation of this type, organizations will need to generate and maintain adequate documentation.

The future Section 3.3 also introduces the requirement to ensure that the collected data is portable and can be made available in a valid format.

---

[1] Bill 64, s. 93; PPIPS, s. 1
[2] Bill 64, s. 93; PPIPS, s. 1
[3] Bill 64, s. 95; PIPPS, s. 3.1 (new provision)
[4] Bill 64, s. 95; PIPPS, s. 3.1 (new provision)
[5] Bill 64, s. 95; PIPPS, s. 3.2 (new provision)
[6] Bill 64, s. 95; PIPPS, s. 3.2 (new provision)
[7] Bill 64, s. 95; PIPPS, s. 3.2 (new provision)
[8] Bill 64, s. 99; PPIPS, s. 8.2 (new provision)

### D. Nature of consent and secondary uses

The Bill also clarifies the concept of consent for the collection and use of personal information.

- Consent must be manifest, free, informed, solicited for specific purposes and separately from any other information provided;

- For sensitive personal information, i.e. information that entails a high level of reasonable expectation of privacy, the consent must be **express**.[9]

- Under the proposed provisions, the secondary use of personal information will be permitted without the prior consent of the person concerned, as long as:

    - the use is for purposes consistent with those for which it was collected (and not for commercial or philanthropic prospection, which are specifically excluded);

    - the use is for the benefit of the person concerned;

    - the use is necessary for study or research or for the production of statistics, and the information is de-identified (i.e. no longer directly identifies the person concerned).[10]

### E. Collection of personal information

The Bill proposes to broaden the information to be disclosed at the time of collection as well as the company's obligations in this regard.

- In addition to specifying the purpose of the collection, the company will need to specify:

    - the means used;

    - the person's right to withdraw consent;

    - where applicable,

        - the name of the third party for whom the data is being collected;

        - the possibility that the information may be transmitted outside Quebec.

- Bill 64 proposes to end the exception provided for in the PPIPS for the collection, use and disclosure of personal information for commercial or philanthropic purposes. In fact, any organization using personal data for such purposes will have to disclose it, and the person concerned will have the option to withdraw his or her consent to such use.[11]

[9] Bill 64, s. 102; PPIPS, ss. 12-13.
[10] Bill 64, s. 102; PPIPS, s. 12
[11] Bill 64, s. 111; PPIPS, s. 22

### F. Collection for profiling purposes

The Bill requires that organizations disclose, in advance, their use of technology that can identify, locate or profile users,[12] and then provide users with the means to disable the identification, location or profiling features.[13]

The following definition for the term "profiling" has been suggested: "*the collection and use of personal information to assess certain characteristics of an individual, in particular for the purpose of analyzing that individual's work performance, economic situation, health, personal preferences, interests or behaviour.*"[14]

### G. Communication to service providers and in the context of commercial transactions

The Bill proposes clarifications to the rules applicable to the disclosure of personal information collected to service providers.

Such disclosure will be subject to certain conditions, including that any such service provider have measures in place to maintain the confidentiality of the information.[15]

The Bill also proposes to fill a significant gap by expressly introducing an exception to allow the release of personal information in the course of a commercial transaction, as permitted under other Canadian laws.[16]

### H. Transfer of information outside Quebec

The Bill reinforces the rules governing the cross-border transfer of personal information by businesses. These rules are currently set out in PPIPS sections 17 and 20.

- Before communication of any information outside Quebec, a business will have to conduct an assessment of the following privacy-related factors:
    - the sensitivity of the information;
    - the purpose for which it will be used;
    - the applicable security safeguards;
    - the legal regime in the jurisdiction, and particularly its degree of equivalence with respect to the principles governing privacy protection in Quebec.[17]

If the assessment shows that the level of data protection would be equivalent to that in Quebec, and subject to the conclusion of a written agreement, the data may be disclosed.[18]

---

[12] Bill 64, s. 99; PPIPS, s. 8.1 (new provision)
[13] Bill 64, s. 99; PPIPS, s. 8.1 (2) (new provision)
[14] Bill 64, s. 99; PPIPS, s. 8.1 (new provision)
[15] Bill 64, s. 107; PPIPA, ss. 18.3 and 18.4 (new provisions)
[16] Bill 64, s. 107; PPIPA, ss. 18.3 and 18.4 (new provisions)
[17] Bill 64, s. 103; PPIPS, s. 17
[18] Bill 64, s. 103; PPIPS, s. 17

For the greater benefit of businesses, the government is following the European Union's approach and has announced that the minister will publish a list of jurisdictions with legal frameworks deemed to be equivalent.[19]

### I. Anonymization and destruction of personal information

The Bill clarifies that organizations may either destroy personal information or anonymize it; the latter option allows organizations to retain information when the purposes for which it was collected or used are achieved (subject to statutory retention periods).[20]

### J. Mandatory notification of data security incidents

The Bill finally introduces mandatory breach notification in the event of a breach of security safeguards involving personal information. Since 2011, the *Commission d'accès à l'information* (CAI) has been recommending such a notification obligation, and this is in keeping with the obligations imposed by the Canadian Parliament and the European Union, both of which adopted mandatory notification programs in recent years.[21]

Here are the key points to bear in mind:

- The term “confidentiality incident” includes:
    - unauthorized access, use or release of personal information;
    - loss of personal information or any other breach in the protection of that information.[22]
- When there is reason to believe that a breach involving personal information has occurred, the organization must take reasonable steps to reduce the risk of injury and to prevent new incidents of the same nature.[23]
- In the event of an incident involving a risk of serious harm, the organization must notify the CAI, as well as any person whose personal information is concerned by the incident.[24]
- To guide businesses in determining the risk threshold, the Bill lists the factors to be considered in assessing the risk of harm:
    - the sensitivity of the information;
    - the anticipated consequences of its use;
    - the likelihood that it will be used for injurious purposes.[25]
- The content and method of the notices will be determined by regulation.[26]

---

[19] Bill 64, s. 103; PPIPS, s. 17.1
[20] Bill 64, s. 111; PPIPS, s. 23
[21] Europe: *General Data Protection Regulation* (May 25, 2018); Canada: PIPEDA and the *Breach of Security Safeguards Regulations* (November 1, 2018)
[22] Bill 64, s. 95; PPIPS, s. 3.6 (new provision)
[23] Bill 64, s. 95; PPIPS, s. 3.5 (new provision)
[24] Bill 64, s. 95; PPIPS, s. 3.5 (new provision)
[25] Bill 64, s. 95; PPIPS, s. 3.7 (new provision)

- All companies must maintain a record of every breach of security safeguards, which must be sent to the CAI upon request.[27] This register can prove very useful in carrying out due diligence on a supplier or an acquisition target.

- The CAI will have the power to order the performance of any measure aimed at protecting the rights granted to affected persons under this law, for the time and under the conditions the Commission determines.[28]

### K. Default configuration

Organizations that collect personal information through technological products or services will now have to ensure that the parameters of the product or service provide the highest level of confidentiality by default. This will entail changes to the digital application deployment process.[29]

### L. Data processing and decisions made using AI

The modernization effort also takes into account the deployment of applications supported by artificial intelligence. The Bill proposes that, when a decision is based exclusively on automated processing, the organization must inform individuals affected by that decision of the parameters used in the decision process and of the procedure for requesting that a staff member review that decision.

### M. Right to de-indexation

Section 28.1 proposes recognizing an individual's right under certain circumstances to require an organization to cease distributing personal information about him or her and to de-index any hyperlink that provides access to that information, particularly if such a distribution contravenes the law or a court order.[30]

A person could also make such a request when the following conditions are met:

- the dissemination of this information causes the person serious injury in relation to the person’s right to respect of his or her reputation or privacy;

- the injury is clearly greater than the public interest in knowing the information or the right to free expression (the balance of convenience criterion);

- the remedy requested does not exceed what is necessary to prevent the perpetuation of the injury.[31]

In assessing the balance of convenience criterion, the following, in particular, must be taken into account:

- the person's notoriety;

- if the person is a minor;

---

[26] Bill 64, s. 95; PPIPS, s. 3.5 (new provision)
[27] Bill 64, s. 95; PPIPS, s. 3.8 (new provision)
[28] Bill 64, s. 144; PPIPS, s. 81.3 (new provision)
[29] Bill 64, s. 100; PPIPS, s. 9.1 (new provision)
[30] Bill 64, s. 113; PPIPS, s. 28.1 (new provision)
[31] Bill 64, s. 113; PPIPS, s. 28.1 (new provision)

- the accuracy of the information being disseminated;
- the sensitivity of the information;
- the context in which the information is disseminated, and the time elapsed between the beginning of the dissemination and the request to halt it.[32]

### N. Release of personal information following a death

The Bill also provides an exception for the release of personal information to a spouse or close relative on the death of a person. This exception to non-disclosure applies when the disclosure is likely to assist the applicant in the grieving process. Furthermore, the deceased person must not have refused such right of access before his or her death.[33]

### O. Penalties

Finally, the Bill's adoption will significantly strengthen corporate accountability by levying hefty fines for violating the law and imposing administrative penalties for failing to meet the obligations specified in the PPIPS.

- First, concerning the administrative penalties, Bill 64 stipulates that these may be imposed, inter alia, when someone collects or uses personal information in contravention of the provisions of PPIPS or fails in his or her duty to report a confidentiality incident.[34]
- Bill 64 gives the CAI a mandate to develop a general framework for the application of these administrative penalties, which should specify the following elements in particular:
    - the objectives associated with the implementation of such a regime;
    - the criteria that must guide the decision-maker in imposing a penalty, including:
        - the seriousness of the violation;
        - the sensitivity of the information;
        - the number of people affected;
        - the measures put in place to remedy the violation;
        - the level of cooperation demonstrated by the organization;
        - the compensation offered to the individuals affected.[35]
- The maximum amount of the administrative penalty is $50,000 (for individuals) and $10,000,000 (for businesses) or, if greater, 2% of worldwide turnover for the preceding year.[36]

---

[32] Bill 64, s. 113; PPIPS, s. 28.1 (new provision)
[33] Bill 64, s. 121; PPIPS, s. 40.1 (new provision)
[34] Bill 64, s. 150; PPIPS, s. 90.1 (new provision)
[35] Bill 64, s. 150; PPIPS, s. 90.2 (new provision)
[36] Bill 64, s. 150; PPIPS, s. 90.12 (new provision)

- Bill 64 also modifies the penal penalties already prescribed in PPIPS and significantly increases their scope. For a corporation, a violation of the PPIPS will result in a fine ranging between $15,000 and $25,000,000 or, if greater, 4% of worldwide turnover for the preceding year.[37] In the event of a subsequent offence, the fines are doubled.[38]

- The offences covered by the penal regime include any collection, possession, release or use of personal information that is contrary to the dictates of PPIPS or any failure to report a confidentiality incident.[39]

### P. Right to private prosecution

Finally, Bill 64 establishes a right for persons affected by an unlawful infringement of the rights conferred by the PPIPS to sue the non-compliant organization for damages. It provides for punitive damages of at least $1,000 to be awarded where the infringement is intentional or the result of gross negligence.[40]

## II. Conclusion

Based on our preliminary analysis, the adoption of the rules proposed in Bill 64 would ensure consistency with the provisions of the *General Data Protection Regulation* (GDPR).

The Bill currently provides for a one-year transition period between its adoption and the coming into force of the new provisions, except for the right to portability, for which the Bill proposes a three-year deferral of implementation.

Given the number of proposed changes and new requirements, such periods are needed to allow companies to review their current practices, identify gaps and implement the necessary changes to ensure compliance.

[37] Bill 64, s. 151; PPIPS, s. 91
[38] Bill 64, s. 151; PPIPS, s. 92.1
[39] Bill 64, s. 151; PPIPS, s. 91
[40] Bill 64, s. 152; PPIPS, s. 91.1