Client Advisory: Bill 64 and Upcoming Changes in Privacy Legislation (Part 1 of 2)

Amy-Lynne Williams, Richard Austin, Fraser Mann, Jennifer Davidson, and Steffi Tran October 12, 2021

Introduction

Privacy in Canada is rapidly evolving. Deeth Williams Wall wants to keep you apprised of the latest changes so you may prepare your organization's compliance activities before legislation comes into effect. This Advisory summarizes actionable elements of the recently passed Québec privacy legislation with commentary on the expected federal privacy legislation.

On September 21, 2021, the National Assembly of Québec adopted Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* ("Bill 64"). Bill 64 will introduce substantial changes to Québec's private sector and public sector privacy legislation. Specifically, a number of important amendments to Québec's *Act respecting the protection of personal information in the private sector* (the "Québec Act") will be incorporated.

Businesses and other organizations located in Québec should take notice of these amendments and change their policies and practices accordingly. Due to the substantial and far-reaching nature of the amendments, we expect that organizations located outside of Québec will also be affected if they conduct business in Québec or collect personal information belonging to Québec residents.

The purpose of this Advisory is to inform you of how the amendments brought on by Bill 64 may affect your operations and aims to enable your organization to act now and prepare your business accordingly before the significant changes come into force.

This is Part 1 of a two-part Advisory that summarizes some of the most significant changes introduced by Bill 64. Part 1 will cover the following topics:

A. the treatment of personal information;
B. the new right of erasure;
C. geolocation; and
D. other notable new obligations for private sector organizations.

Part 2 of our Advisory will be released shortly and will address:

A. data profiling;
B. de-identification and anonymization of personal information;
C. artificial intelligence/automated processing; and
D. the new enforcement regime and the penalties that apply.

In addition, the federal Bill C-11, the *Digital Charter Implementation Act, 2020* ("Bill C-11") underwent its first reading before Parliament was prorogued for the September 2021 election. Bill C-11 also proposes to introduce substantial changes to modernize current privacy laws in Canada. We anticipate that Bill C-11 or a revised version of it will be introduced in the next session of Parliament. In order to best prepare your organization for the anticipated changes, we have provided a brief update on relevant changes to federal privacy legislation under Bill C-11 after each topic discussed in this Advisory.

We expect the obligations imposed by Bill 64 will set some of the most stringent privacy protection standards in the country. On that basis, it would be prudent for your organization to prepare to implement privacy changes in accordance with the amendments brought on by Bill 64. Doing so will protect your organization if you handle personal information of end-users from

Québec and will best prepare you for compliance with future federal or provincial amendments to privacy legislation.

Bill 64 received Royal Assent on September 22, 2021. The implementation period of the new requirements imposed by Bill 64 began on that date. Certain provisions will enter into force one, two, or three years after September 22, 2021, as indicated below.

A. New Requirements When Dealing with Personal Information

Bill 64 contains a number of heightened consent requirements that organizations will have to comply with in the course of collecting personal information from individuals. In this section, we discuss:

- enhanced collection and consent obligations;
- sensitive personal information; and
- exceptions to consent.

i) Enhanced Collection and Consent Obligations (Coming into Force September 22, 2023)

Previously, under Section 8 of the Québec Act, organizations collecting personal information had to inform the individual whose information was being collected of:

- the object of the file;
- how the personal information would be used and the categories of persons who would have access to the information within the enterprise; and
- the place where the file would be kept and rights of access and rectification.

Under Bill 64, Section 8 of the Québec Act will be amended to require organizations collecting personal information to inform the individual (upon collecting the information and subsequently upon request) of:

- the purposes for which the information is collected;
- the means by which the information is collected;
- the rights of access and rectification provided by law; and
- the individual's right to withdraw consent to the communication of the information or to withdraw consent to the use of the information.

In the event that information is collected on behalf of a third party, the amendments will also require organizations to inform the individual of "the name of the third [party] for whom the information is being collected, the names of the third [party] or categories of third [partie(s)] to whom it is necessary to communicate the information…and of the possibility that the information could be communicated outside Québec".

Section 14 of the Québec Act previously required consent to be:

> "manifest, free, and enlightened, and must be given for specific purposes".

Under Bill 64, Section 14 of the Québec Act will be amended to require that consent be:

> "clear, free and informed and be given for specific purposes".

The amendments will also require organizations to request consent for each purpose, in clear and simple language. When the request for consent is made in writing, it must be presented separately from any other information provided to the person concerned. This means that consent for the collection of personal information must be handled as a standalone request.

Steps to Take:

Organizations should begin reviewing current policies and practices relating to the acquisition of consent when collecting personal information and update or replace such policies and practices accordingly. New or updated policies should prepare for and implement processes to enable the organization to respond effectively to individuals requesting information about how the organization handles their personal information.

ii) Sensitive Personal Information (Coming into Force September 22, 2023)

Bill 64 introduces the term "sensitive personal information" and will require organizations to obtain express consent if the information concerned is "sensitive personal information".

Sensitive personal information is defined under Section 12 of the Québec Act as personal information which, due to its nature or context of its use or communication, "entails a high level of reasonable expectation of privacy". This includes medical, biometric or otherwise intimate information. In addition, as facial recognition technology involves the collection and processing of biometric data, such information will be considered "sensitive personal information".

Steps to Take:

Organizations should become familiar with the concept of "sensitive personal information", examine the type of information they are collecting, and identify whether such information may be categorized as "sensitive personal information".

iii) Exceptions to Consent (Coming into Force September 22, 2023)

In certain situations, organizations will be allowed to use personal information for alternate purposes without additional consent from the individual(s) concerned.

Specifically, Section 12 of the Québec Act will introduce new exceptions to consent.

Under Section 12, organizations can use personal information for another purpose if:

- it is consistent with the purposes for which the information was collected;
- it is "clearly used for the benefit of the person concerned", such as when its use is necessary for fraud prevention and detection or the evaluation and improvement of protection and security measures, or the supply or delivery of a requested product or provision of a service; or
- the information is de-identified and it is necessary for study purposes, research purposes, or the production of statistics.

Steps to Take:

Organizations should become familiar with these new exceptions and review existing agreements with third parties who receive personal information, ensuring that the terms comply with or will be amended to comply with the new legislative requirements.

Comparison with Bill C-11

Bill C-11 also proposes heightened consent obligations, such as requiring organizations to inform individuals in plain language of the purpose of the collection, use, or disclosure of their personal information and the ways such information may be shared with third parties. Bill C-11 may also require organizations to provide information regarding any "foreseeable consequences" to the collection, use or disclosure of personal information, although the term "foreseeable consequences" has not yet been defined.

For additional information on Bill C-11's proposed requirements relating to consent and the collection, use, and disclosure of personal information, please see our previous two-part commentary here and here.

B. Geolocation

Requirements on Cross-Border Data Transfers (Coming into Force September 22, 2023)

Section 17 of the Québec Act will require organizations to "conduct an assessment of privacy-related factors" before communicating personal information outside Québec. Specifically, the organization must consider:

- the sensitivity of the information;
- the purposes for which the information is to be used;
- the protection measures, including contractual measures, that would apply; and
- the legal framework applicable in the State in which the information would be communicated, including applicable data protection principles.

The personal information may be communicated outside Québec if the assessment shows that the information would receive "adequate protection in compliance with generally accepted data protection principles."

The communication of the information must also be the subject of a written agreement that considers the results of the assessment and, if applicable, the terms agreed on to mitigate any identified risks.

Steps to Take:

Organizations must be aware that compliance with Section 17 of the Québec Act is necessary even when they have entrusted a person or body outside Québec with the task of collecting, using, communicating or keeping such information on the organization's behalf.

The phrase "generally accepted data protection principles" has not yet been further defined and therefore organizations should become familiar with the use of such assessments, properly document relevant practices, and continue to monitor for the release of additional guidance or interpretation.

Comparison with Bill C-11

Bill C-11 proposes to require organizations to make readily available information on whether it carries out any international or interprovincial transfer or disclosure of personal information that may have "reasonably foreseeable privacy implications". However, there is currently limited guidance on this cross-border data transfer requirement. For additional information, please see our previous commentary here.

C. Introduction of New Right of Erasure

Rights to Erasure, De-Indexation, and Re-Indexation (Coming into Force September 22, 2023)

Section 28.1 of the Québec Act will introduce a new right of erasure. Individuals will gain the right to require any person carrying on an enterprise to cease disseminating their personal information or to de-index any hyperlink to such information if the dissemination of the information contravenes the law or a court order.

Section 28.1 also provides that individuals may require any person carrying on an enterprise to cease disseminating their personal information, de-index any hyperlink to such information, or re-index any hyperlink to such information where the following conditions are met:

- the dissemination of the information causes the person concerned serious injury in relation to his right to the respect of his reputation or privacy;
- the injury is clearly greater than the interest of the public in knowing the information or the interest of any person in expressing himself freely; and
- the cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary for preventing the perpetuation of the injury.

Steps to Take:

Organizations need to review current policies and protocols, such as procedures regarding how requests to dispose of information will be handled, in order to ensure compliance with these anticipated take-down, de-indexing, and re-indexing provisions.

Comparison with Bill C-11

Bill C-11 also proposes to create a new right for individuals to request an organization to dispose of (i.e., permanently delete) their personal information that the organization has collected. However, Bill C-11 does not go as far to require organizations to de-index or re-index personal information. The new right to disposal/erasure proposed by Bill C-11 appears to be less stringent than the rights outlined under Bill 64. For more information, see our previous commentary on Bill C-11 here.

D. Additional Obligations for Organizations

Organizations may need to make substantial changes to existing policies and procedures in order to fulfill the new obligations introduced by Bill 64. A number of notable changes include:

- the requirement to designate a person in charge of protection of personal information;
- the obligation to implement a privacy management program;

- the obligation to conduct privacy impact assessments;
- mandatory notifications of privacy breaches;
- privacy by design/privacy by default requirements; and
- the new right to data mobility/portability.

i) Requirement to Designate a Person in Charge of Protection of Personal Information (Coming into Force September 22, 2022)

Under Section 3.1 of the Québec Act, organizations will be required to designate a person in charge of the protection of personal information and make their title and contact information available by an appropriate means (i.e., publishing this information on the organization's website).

This responsibility defaults to the "person exercising the highest authority" within the organization. However, that individual may delegate all or part of "the function of the person in charge of the protection of personal information" to "any person", so this function can be delegated to an individual internal or external to the organization.

Steps to Take:

As this provision comes into force only one year after the date of Bill 64's assent, organizations should begin the selection process to designate an appropriate individual to be responsible for the protection of personal information, and to publish their contact information soon after. That individual must become familiar with their obligations and may consider delegating their functions.

ii) Obligation to Implement a Privacy Management Program (Coming into Force September 22, 2023)

Section 3.2 of the Québec Act introduces an obligation to "establish and implement governance policies and practices regarding personal information that ensure the protection of such information".

Specifically, organizations must ensure that their policies and practices outline a framework for the retention and destruction of personal information; provide a complaint process regarding the protection of information; and define the roles and responsibilities of their personnel throughout the life cycle of personal information.

The policies and practices must also be "proportionate to the nature and scope of the enterprise's activities" and be approved by the person designated to be in charge of the protection of personal information.

Organizations will also need to publish their policies and practices in clear and simple terms and make them available by an appropriate means (i.e., publishing on the organization's website).

Steps to Take:

Organizations should review their current policies and practices, update or replace them accordingly in light of these new obligations, and make them available for viewing.

iii) Obligation to Conduct Privacy Impact Assessments (Coming into Force September 22, 2023)

Section 3.3 of the Québec Act will require organizations to conduct a privacy impact assessment upon the:

> "acquisition, development and redesign of an information system or electronic service delivery involving the collection, use, communication, keeping or destruction of personal information".

The privacy impact assessments must be "proportionate" to the sensitivity of the personal information, purpose of use, amount, distribution, and format of the information.

Privacy impact assessments are also required when communicating personal information outside Québec, as discussed in the "Geolocation" topic above.

Steps to Take:

Organizations should familiarize themselves with the use of privacy impact assessments and begin preparing and developing procedures that will demonstrate compliance with these new obligations.

iv) Mandatory Notifications of Privacy Breaches (Coming into Force September 22, 2022)

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

Section 3.6 newly defines "confidentiality incident" as:

- access not authorized by law to personal information;
- use not authorized by law of personal information;
- communication not authorized by law of personal information; or
- loss of personal information or any other breach in the protection of such information.

Under Section 3.5, an organization that has cause to believe that a confidentiality incident has occurred must take reasonable measures to reduce the risk of injury and prevent future incidents of the same nature.

The organization must promptly notify the Commission d'accès à l'information (CAI) and any person whose personal information is concerned by the incident if the incident "presents a risk of serious injury". However, an organization would not be required to notify such a person "if doing so may hamper an investigation conducted by a person or body responsible by law for the prevention, detection or repression of crime or statutory offences".

In addition, Section 3.5 states that organizations may notify any person or body that could reduce the risk of serious injury, by communicating to the person or body only the personal information necessary for that purpose without the consent of the person concerned.

Section 3.7 outlines the considerations that organizations must take into account in assessing the risk of injury to a person whose personal information is concerned by a confidentiality incident. Such considerations include the sensitivity of the information concerned, the

anticipated consequences of its use, and the likelihood that such information will be used for injurious purposes.

Lastly, under Section 3.8, organizations will be required to maintain a register of confidentiality incidents, a copy of the which must be sent to the CAI upon request.

Steps to Take:

Many organizations are already familiar with the breach reporting requirements under the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). For those who are not, since this provision comes into force only one year after the date of Bill 64's assent, organizations should begin reviewing any current security incident response processes and update or replace such processes to comply with these new requirements in the event of a "confidentiality incident".

Given the mandatory reporting requirements of "confidentiality incidents" under Bill 64 and "breaches in security safeguards" under PIPEDA and the different ways they are defined, organizations should familiarize themselves with the obligations under each statute and prepare their breach reports accordingly. Depending on the circumstances, an organization may have to report under one or both of the statutes.

v) Privacy by Design/Privacy by Default Requirements (Coming into Force September 22, 2023)

Section 9.1 of the Québec Act introduces the principle of privacy by default.

Organizations will have to ensure that, by default, the parameters of the technological product or service offered to the public provide "the highest level of confidentiality without any intervention by the person concerned".

This section would thus apply if the organization offered products or services with privacy settings, such as social networking accounts, search engines, mobile applications, etc.

This requirement does not apply to the privacy settings of cookies.

Steps to Take:

Organizations should design products or services for privacy and assess privacy risks at the start of the planning process. Organizations should be aware that there is currently still uncertainty regarding what will constitute the "highest level of confidentiality" when offering a technological product or service.

vi) New Right to Data Mobility/Portability (Coming into Force September 22, 2024)

Section 27 of the Québec Act provides individuals with a new right to data portability.

Individuals may request that an organization holding their personal information confirm the existence of, communicate, and provide a copy of the personal information.

The computerized personal information must be provided in the form of a written and intelligible transcript.

Section 27 also states that "computerized personal information collected from the applicant, and not created or derived from personal information about the applicant", must be communicated in a "structured, commonly used technological format" upon request, unless doing so raises serious practical difficulties.

Steps to Take:

Organizations should begin to update or create policies and practices that will enable them to respond effectively and provide personal information held on an individual in an appropriate format upon that individual's request.

The purpose of this new right is to enable individuals to be able to retrieve the information they have provided to the business – and nothing more.

Organizations should not misconstrue this right as a requirement that they must share data produced using proprietary methods with their competitors.

Comparison with Bill C-11

While Bill C-11 does not explicitly require organizations to designate a person in charge of personal information or conduct privacy impact assessments, it proposes to introduce an obligation on organizations to implement a privacy management program. Such a program must include certain policies, practices, and procedures directed at fulfilling obligations such as:

- protecting personal information;
- responding to requests for information and complaints;
- training and communicating to staff information about the organization's policies and practices; and
- developing external materials to explain the organization's policies and procedures.

Bill C-11's mandatory breach reporting obligations will likely be in line with those outlined by PIPEDA, generally.

However, the penalties of violating those obligations will be more significant, and these will be discussed in Part 2 of this Advisory.

In addition, while Bill C-11 does not outline explicit privacy by design or by default requirements like Bill 64, the Office of the Privacy Commissioner of Canada has previously endorsed the use of privacy by design requirements to increase accountability.

Lastly, similar to Bill 64, Bill C-11 also introduces a new right to data mobility/portability.

For more information on the new amendments proposed by Bill C-11, please see our previous commentary here and here.

Concluding Comments

Bill 64 will introduce substantial changes to modernize current privacy laws in Québec and will likely have far-reaching effects on private sector organizations that conduct business in Québec.

Part 1 of this Advisory has provided an overview of upcoming changes, including new requirements regarding the collection of personal information, the new right of erasure, geolocation, and additional obligations on organizations.

Bill 64 will also affect areas such as data profiling, de-identification and anonymization of personal information, artificial intelligence/automated processing, and will impose a new enforcement regime. We will soon publish Part 2 of this Advisory, which will discuss these changes further and provide additional guidance.

If you have further questions, please contact a member of our information technology group.

Amy-Lynne Williams

Richard Austin

Fraser Mann

Elisabeth Symons

Olalekan (Wole) Akinremi

Jennifer Davidson

Anna Troshchynsky

M. Imtiaz Karamat

Steffi Tran