Privacy Impact Assessments (PIAs) and Other Assessments

Quebec's Private Sector Privacy Law Amendments C. 25
Sections 3.3 and 3.4, 17 and 21

Introduction

On September 22, 2021, Quebec passed *An Act to modernize legislative provisions as regards the protection of personal information* (2021, c. 25) ("the Act") updating public and private sector privacy laws. The provisions of the Act come into force over a period of 3 years.

This document was created by leading Canadian privacy experts working with national and regional industry associations. We believe a harmonized approach to privacy law across Canadian jurisdictions is important so that the rules are understandable for individuals and enterprises. Interpretations of privacy laws should be pragmatic, reasonable and focus on the privacy outcomes for individuals and practical implementation for enterprises. With this in mind, we have created what we think is appropriate guidance for interpreting some of the more challenging provisions of the Act.

This document can be shared and used by enterprises. This is not legal advice; it is suggested best practices for entities wishing to work pragmatically on their compliance with the Act before any additional guidance from the *Commission d'accès à l'information* (the "CAI") or regulations are made available. We encourage enterprises to monitor developments in CAI and government guidance on these and other topics related to the Act.

Privacy Impact Assessments (PIAs)

Conducting PIAs when processing personal information has been a best practice for many years in Canada. The Act now formally requires enterprises to conduct a PIA in certain circumstances.

a) Which activities require a PIA? (s. 3.3 para. 1)

A PIA will be required for "*any project to acquire, develop or overhaul an* ***information system or electronic service delivery system*** *involving the collection, use, disclosure, retention or destruction of personal information.*" This would include both internal projects or those involving external parties. A substantial update to an existing system (e.g., a document management platform) could be considered an "overhaul" and will therefore require a PIA. Additional considerations include:

- **Conducting an assessment** (s. 3.3 para. 4) The PIA must be proportionate to the:
  - sensitivity of the information concerned;
  - purpose for which the information is to be used;
  - quantity and distribution of the information; and
  - medium on which it is stored.

Ensuring the PIA is proportionate is intended to ensure that the scope of the PIA is appropriate to the risk or impact of the project on the individuals' right to privacy. For example, a project involving minimal personal information, which is not very sensitive, would not require the same type of PIA as the implementation of a biometric system involving a large number of individuals.

- **Consulting with the Privacy Officer** (s. 3.3 para. 2 and s. 3.4) The Privacy Officer (or their delegate) should be consulted early on and may, at any stage of the project, suggest personal information protection measures that should be applied to the project. This is consistent with best practices today and existing processes can likely be relied upon. The consultation and protection measures should be risked based. For example, protection measures could include:
  - appointment of a person to be responsible for implementing personal information protection measures;
  - measures to protect personal information in any document relating to the project;
  - a description of the project participants' responsibilities regarding the protection of personal information; or
  - training activities for project participants on the protection of personal information.
- **Communicating data [aka limited data portability]** (s. 3.3 para.3) Enterprises must make sure these projects can accommodate requests from individuals to receive their computerized personal information in a structured and commonly used technological format – an expanded access right for individuals. Remember:
  - data in digital format, not paper
  - data collected from the individual, not data generated by the enterprise or collected form 3rd parties
  - data is to be communicated to the individual, or to any other third party authorized by law
  - communicated in a structured, commonly used technological format, e.g.
    - could provide data in similar format used for collection (jpeg in, jpeg out)
    - could be a very broad spectrum of possibilities (pdf, excel, csv, etc.)

b) Examples of projects likely covered by the PIA requirement

Note that the CAI's current guide on PIAs provides useful tools for enterprises that want to become familiar with the process (*Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privée* - available in French only, updated in March 2021). The CAI has indicated it will revise this guide in light of the Act.

In this guide, the CAI recommends that a PIA be conducted for any project involving personal information. While this is a much broader requirement than the one set out in the Act, it is still interesting to highlight some of the types of projects that the CAI believes may be covered:

- developing a new information system or a personalization feature for a product or service

- searching for new customers, exploring new markets
- using an algorithm or an artificial intelligence system
- installing a video surveillance system
- comparing different versions of databases or files
- acquiring or merging organizations
- using fingerprints, geolocation, facial recognition, connected objects, smart city sensors, etc.

c) Other types of activities requiring some form of assessment:

- **Cross-border transfers (s. 17)** An enterprise that:
  - wishes to transfer personal information outside Québec, or
  - entrusts a third party (including an affiliate) located outside Québec with the task of collecting, using, disclosing or keeping personal information on its behalf,

  is required to:
  - conduct an assessment, and
  - enter into a written data transfer agreement with the cross-border recipient before transferring the personal information.

*See **Cross-border Transfers** for the privacy-related factors to consider in performing the assessment and suggested key contractual provisions to include in the agreement as a best practice.*

- **Research projects (s. 21)** The amendments to section 21 and the introduction of new sections 21.0.1 and 21.0.2 replace the current process with a new regime. Parties to a transfer of personal information for research purposes can now make the assessment themselves. The information may be communicated if the assessment concludes that:
  - the personal information is needed to achieve the objective;
  - it is unreasonable to require the requesting person or body to obtain consent;
  - the objective of the research outweighs the impact on individual privacy in light of the public interest;
  - the information is used in a manner that ensures its confidentiality; and
  - only necessary information is communicated (s. 21 para. 2).