Cross-border Transfers

Quebec's Private Sector Privacy Law Amendments C. 25
Section 17

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.

Cross-border Transfers

The Act requires an enterprise (including its service provider, corporate affiliate, or corporate department outside of Quebec) to meet the following requirements before it can transfer personal information outside of Quebec:

1) Conduct an assessment of privacy-related factors that establishes that the information would receive an adequate protection in compliance with generally accepted data protection principles; and

2) Enter into a written agreement that takes into account the results of the assessment and, if applicable, include terms that mitigate the risks identified in the assessment.

It may be helpful to reference the Office of the Privacy Commissioner of Canada's guidelines for processing personal data across borders.

a) Privacy-related factors that must be assessed

Enterprises must consider the following privacy-related factors and satisfy itself that the information would be protected in compliance with generally accepted data protection principles.

1) Sensitivity of information: "Intimate" information, including medical, biometric or where the context or its use or disclosure entails a high level of reasonable expectation of privacy, is subject to a higher degree of protection.

2) Purposes for which it is to be used: The information being transferred must be reasonably required for the identified purposes.

3) Protection measures, including contractual ones, to be applied: The protection measures must be appropriate to the sensitivity of the information and should take into account the likely risk of and potential impact of unauthorized access to, use or disclosure of, the information.

4) Legal framework applicable in the recipient jurisdiction: The data protection laws of the foreign jurisdiction should protect the information in compliance with generally accepted data protection principles. It would be commercially reasonable to assess a destination state's legal framework against the OECD principles which form the basis of most of the leading data protection laws around the world

b) Written agreement for data transfer

Once the enterprise completes the assessment and determines that the information may be transferred to the destination state, the enterprise must then enter into a written data transfer agreement with the cross-border recipient. The agreement should take into account the results of the assessment and, if applicable, include any terms required to mitigate the risks identified in the assessment.

The following key contractual provisions are suggested as a best practice to assist in compliance with this requirement:

Section 1 – Purpose and Scope

Clearly define the purposes and scope for which the service provider can process the data, and strictly limit all processing to those purposes.

Section 2 – Interpretation

The definitions or terminology used in data protection laws, or in common parlance, may differ between jurisdictions. It is therefore recommended to have a definitions section to ensure certainty of interpretation, focusing in particular on clarifying key terms where differences in terminology may exist, such as with respect to defining what is sensitive information.

Section 3 – Obligations of the parties

- **Limited purpose.** Service provider can only process the data in accordance with instructions and for the specified purposes.

- **Accuracy and Transparency.** Service provider must inform customer when it becomes aware of inaccurate data and work with customer to rectify.

- **Cooperation.** Service provider must cooperate with and assist customer in compliance with applicable privacy legislation including access requests, data portability, data deletion, complying with requests from privacy regulators

- **Security incident.** Service provider must inform customer when it becomes aware of a security breach involving the customer's personal information, address breach and mitigate adverse effects, work with customer to assess breach and notify affected individuals and regulators as needed.

- **Return or Destruction of personal information.** Service provider must destroy or return data as instructed by customer or upon expiration of the agreement

- **Security measures.** Service provider must protect the data using safeguards appropriate to the level of sensitivity of the data. For example:

    - Restrict access to need to know, access control and data segregation;

    - Security screening of employees; and

    - Oversight and monitoring of privacy safeguards.

Requiring adherence to a detailed standard is recommended. Such standards could be set out by the enterprise in an appendix, or the contract could require compliance with one or more recognized external security standards.

- **Policy and Procedures.** Service provider must have privacy and security related policies and procedures or comply with customer's privacy and security policy and procedures.

- **Training and Quality**. Service providers must have mandatory privacy training for employees and have a mechanism to track the completion of training upon hiring and on a continual basis.

- **Notification**. Service provider must inform the customer when local laws and practices may impact the contract.

Section 4 - Third-party and Subcontractors.

Service provider cannot transfer the data to a third party (including subcontractors) or transfer data outside of the permitted jurisdiction(s) without the organization's written consent. It is also possible to allow for a transfer to a pre-defined party, or group of parties (following an assessment by the enterprise), but prohibit transfers to other third parties without the transferring/controlling organization's consent.

Section 5 – Quality Control

- **Audit.** Customer may audit service provider's compliance with privacy and security obligations. Customer may conduct audit by itself or through independent auditor.

- **Documentation and Compliance.** Service provider must maintain appropriate documentation to be able to demonstrate its compliance with the contract, applicable laws and best practices.

Section 6 – Access request from Government and other public authorities

To the extent permitted by law, Service provider must notify customer in the event that it receives an access request, production order, subpoena of similar request, demand or order from a governmental or other public authority and shall provide reasonable assistance to the organization should the organization to seek a protective order.

Section 7 – Governing Law

If possible, governing law should be the laws of the province of Quebec.

Section 8 – Liability and Insurance

- Service provider shall be liable for and shall indemnify customer for losses related to a privacy or security breach.

- Service provider shall maintain cyber liability insurance subject to a limit of not less than [X million per occurrence, amount to be determined by risk assessment].