Cross-border transfers of personal information outside Québec: new requirements for businesses

December 06, 2022

The *Act to modernize legislative provisions as regards the protection of personal information* (the Amended Act), adopted on September 21, 2021, makes significant changes to the rules applicable to the communication of personal information outside Québec (specifically, the sharing of information or the granting of remote access, both of which we will refer to as transfers), whether the transfers are to a service provider or to some other category of third party. In this article, we describe the new Québec framework governing international and interprovincial transfers of personal information and provide compliance tips to organisations.

Legal framework applicable to transfers of personal information

Prior to the adoption of the Amended Act, section 17 of the *Act respecting the protection of personal information in the private sector* (the ARPPIPS) stated that, with regard to the communication of information outside Québec, enterprises must "take all reasonable steps" to ensure that the information will not be used for purposes other than those for which consent has been obtained and will not be disclosed to third parties without the consent of the persons concerned. In the case of nominative lists, that Act required that the persons concerned be given the opportunity to refuse the use of their personal information for purposes of commercial or philanthropic prospecting. Enterprises were required to refuse to communicate the information if these conditions were not met.

Effective September 22, 2023, a new obligation of transparency, set out in paragraph 2 of a new section 8, will require enterprises to notify the person concerned, at the time of collection and subsequently on request, of the possibility that the information collected may be communicated outside Québec.

Furthermore, the new section 17 modifies the framework governing transfers and provides that:

> Before communicating personal information outside Québec, a person carrying on *an enterprise must conduct a* ***privacy impact assessment*** *. The person must, in particular, take into account*
>
> *(1) the sensitivity of the information;*
>
> *(2) the purposes for which it is to be used;*
>
> *(3) the protection measures, including those that are contractual, that would apply to it; and*
>
> *(4) the legal framework applicable in the State in which the information would be communicated, including the personal information protection principles applicable in that State.*
>
> *The information may be communicated if the assessment establishes that it would receive adequate protection, in particular in light of generally recognized principles regarding the protection of personal information. The communication of the information must be the subject of a written agreement that takes into account, in particular, the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment.*
>
> *The same applies where the person carrying on an enterprise entrusts a person or* body outside Québec with the task of collecting, using, communicating or keeping *such information on his behalf.*

The purpose of these new requirements is to ensure an adequate level of protection for information transferred outside the province. At the clause-by-clause consideration stage, the adequacy standard was adopted in place of the equivalency standard, which is regarded as stricter.

Thus, in order for a transfer to be authorized by the Amended Act, the exporting enterprise needs to conduct a privacy impact assessment in relation to the proposed transfer. It must then ensure that the protective measures in place will adequately protect the exported information. The measures must include a written contract with the entity receiving the information.

Transfer impact assessments

An enterprise that (1) wishes to communicate personal information outside Québec or (2) entrusts a third party outside Québec with the task of collecting, using, releasing or keeping personal information on its behalf must, commencing in September 2023, carry out a privacy impact assessment prior to the transfer (a Transfer Impact Assessment or TIA). This TIA must take the following factors into account:

- the sensitivity of the information;
- the purposes for which it is to be used;
- the protective measures, including the contractual measures, that would apply to the communication; and

- the legal framework applicable in the State in which the information will be released, including the personal information protection principles applicable in that State.

This last factor raises several questions in the absence of guidance from the Commission d'accès à l'information. The analysis of the legal framework of the receiving jurisdiction has been a matter of extensive commentary since the Court of Justice of the European Union (CJEU) decision in Schrems II. Several stakeholders are concerned that such restrictions could adversely affect the province's economy by restricting information flows. On the date of this article, the following elements should, in our opinion, be taken into account:

- The TIA must assess the foreign legal framework in light of "generally recognized principles regarding the protection of personal information." This amendment, which was drafted during the clause-by-clause consideration of the Bill, refers to the principles adopted by the Organization of Economic Cooperation and Development (OECD) in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted in 1980 and updated in 2013 (the OECD Guidelines). They are also reflected in the foreign law analytical grid issued by Québec's Secrétariat à la réforme des institutions démocratiques, à l'accès à l'Information et à la laïcité to help public bodies implement section 70.1 of the amended Act Respecting Access, whose wording is identical to the wording of section 17 of the Amended Act. Those principles are as follows: (i) collection limitation; (ii) data quality; (iii) purpose specification; (iv) use limitation; (v) security safeguards; (vi) openness; (vii) individual participation; and (viii) accountability. In the absence of regulatory guidance regarding section 17, it seems reasonable to use this analytical grid in the context of TIAs under the Amended Act.
- In our opinion, analysis of the legal framework of the receiving jurisdiction should also include an assessment of the enforceability of the contractual protective measures (described below). Indeed, if public order laws or overriding mandatory laws of the receiving State prevent the enterprise from enforcing the contractual protection measures (for example if the foreign legal framework governing oversight denies the protection required by the OECD Principles), or would result in denying the execution of a Québec judgment that seeks to enforce the contract, the protection offered by the receiving State would not in all likelihood be considered adequate.
- The matter of the frequency of TIAs is up in the air for the moment, as the Amended Act does not contain specific requirements to that effect. Given the influence of the EU General Data Protection Regulation (GDPR) on the Amended Act, it is possible that the legislator is anticipating that enterprises will carry out regular legislative monitoring of the jurisdictions where information will be transferred so that their TIAs can be updated in a manner consistent with the recommendations of the European Data Protection Board in its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Implementation of protective measures, including contractual measures

Section 17 also requires that the TIAs take into account the protective measures, including the contractual measures, that would apply to the transfer of personal information. The Québec legislator has indeed chosen to rely mainly on the contractual route when it comes to providing an adequate level of personal information protection. In this regard, a distinction should be made between transfers to service providers (who can use the information solely on behalf and for the benefit of their client) and transfers to other third parties.

Service providers

Where the transfer is to a service provider, section 18.3 of the Amended Act requires that a written contract be entered into and that it:

- specify the measures that the service provider must take to protect confidentiality, to ensure that the information is used only for carrying out the mandate or performing the contract and to ensure that the service provider does not keep the information after the expiry of the contract;
- state that the service provider must notify the person in charge of the protection of personal information (*e.g.* the privacy officer of the client company), without delay, of any violation or attempted violation by any person of any obligation of confidentiality; and
- state that the person in charge of the protection of personal information must be permitted to carry out any verifications relating to the service provider's confidentiality obligations.

In addition to these provisions specific to service contracts, the contract must take into account the results of the TIA. If, based on the TIA, it can be concluded that the information processed abroad by a service provider will be sufficiently protected with a contract that simply incorporates the requirements of section 18.3, no other measure will be necessary for the transfer to proceed.

If however the TIA indicates that processing abroad poses a risk for the protection of the information, the parties must, in their contract, implement and document measures that reduce the risk to an adequate level. In our view, technical measures (such as encryption and depersonalization) and organizational measures (such as corporate policies restricting the sharing of information with foreign government authorities) should be considered, consistent with the supplementary measures articulated by the European Data Protection Board in Recommendations 01/2020.

Other recipients

Although the Amended Act does not impose any specific contents for contracts applicable to the sharing of information with third parties outside Québec that are not acting as service providers (such as potential acquirers of a company's assets, or affiliates that intend to use the data for their own purposes), we believe the following obligations flow from the requirements of section 17:

- a written contract must be entered into with each such recipient;
- the contract must provide an adequate level of protection for the transferred information by incorporating, among other things, the obligations stemming from the OECD Principles (limited collection, data quality, purpose specification, use

limitation, protection safeguards, openness, individual participation, and accountability); and
- the parties must take into account the results of the TIA and, if applicable, put in place measures to reduce to an adequate level the risks associated with the foreign legal regime. This analysis should use the same criteria that are used in the context of a transfer to a service provider.

Differences with the federal framework

In 2009, the Office of the Privacy Commissioner of Canada (OPC) published its Guidelines for processing personal information across borders, in connection with the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The guidelines require organizations that transfer personal information for processing purposes to provide, by contractual or other means, "a **comparable** level of protection while the information is being processed by the third party." Such organizations are also subject to an obligation of transparency, which requires them to notify the individuals concerned that information is being transferred outside Canada, and that there is a risk foreign authorities may access it.

In the case of outsourcing to another jurisdiction, the OPC guidelines state that PIPEDA *does **not*** require a measure by measure comparison of foreign laws with Canadian laws. It *does* however require organizations to "take into consideration all of the elements surrounding the transaction." Interestingly, the OPC recently applied these guidelines in PIPEDA Findings 2020-0001 pursuant to its investigation into an outsourcing agreement between a Canadian financial institution and a supplier in India in connection with fraud claim processing services. The takeaway from these findings pertains to the risk analysis done by the financial institution. The OPC approved of that analysis, concluding that the following protection measures were appropriate under the circumstances:

- a privacy impact assessment with respect to the planned outsourcing was carried out;
- legal advice concerning India's legal framework governing privacy and information protection was obtained; and
- the findings of these risk assessment activities were incorporated into the contract with the service provider, which included detailed organizational and technical measures to protect the information to be processed.

The recent PIPEDA reform bill introduced by the federal government in June 2022 (Bill C-27) merely imposes an obligation of openness and transparency with regard to international and interprovincial transfers. The organization's external privacy policy will need to specify whether or not it will carry out any international or interprovincial transfer or disclosure of personal information that may have "reasonably foreseeable privacy implications" (Bill C-27, s. 62(2)(d)). This requirement comes on top of the outsourcing obligations, which provide, among other things, that the organization must ensure, contractually or by other means, that the service provider offers a level of protection equivalent to what the organization is required to offer for such personal information under Bill C-27.

Compliance tips

Since the requirements of the Amended Act governing transfers outside Québec will soon be in force, organizations should put in place the following measures:

- Map out the flows of personal information, the jurisdictions to which such information will be exported, and the categories of recipients who will import and process such information.
- Develop a TIA template for analyzing the legal frameworks of the importing jurisdictions having regard to the OECD Principles. The analytical grid prepared by the Québec government for public sector bodies can be used as the reference for this exercise.
- Identify the jurisdictions where the organization will be transferring personal information. If their legal regime risks contravening the OECD Principles, assess whether contractual, organizational and technical measures could reduce the risk to an acceptable level by providing adequate protection for the transferred information.
- Ensure that the relevant contracts include personal information transfer clauses that comply with the new requirements, having regard to the circumstances under which the transfers are to be made.

Contact us

BLG's Cybersecurity, Privacy & Data Protection Group keeps a close eye on developments that could help businesses better understand the new requirements in the Amended Act with regard to interprovincial and international transfers of personal information. Our team helps businesses implement the required compliance measures.

The authors would like to thank Cassandre Legault, student-at-law, for her contribution in writing this article.

By

Elisa Henry, Anthony Hémond

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749