# Cross-border transfers of personal information outside Québec: Requirements for businesses

**May 07, 2024**

***This updated article was originally published in December 2022*** .

The Québec *Act respecting the protection of personal information* (the ARPPIPS), provides significant obligations when communicating 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 Québec framework governing international and interprovincial transfers of personal information, and provide compliance tips to organisations.

## Legal framework applicable to transfers of personal information

Since September 22, 2023, an obligation of transparency, set out in paragraph 2 of section 8 of the ARPPIPS, requires organizations 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.

This notification is usually done by the organization in its customer- and employee-facing privacy policies.

Furthermore, section 17 modifies the framework governing transfers and imposes additional requirements on organizations to ensure an adequate level of protection for information transferred outside the province.

In order for a transfer to be authorized by the ARPPIPS, the exporting organization needs to conduct a privacy impact assessment in relation to the proposed transfer (a Transfer Impact Assessment, or TIA). It must then ensure that the protective measures in place will adequately protect the exported information. These measures must include a written contract with the entity receiving the information.

## Transfer impact assessments

An organization 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 carry out, prior to the transfer, a TIA that takes 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 information; and
- the legal framework applicable in the State in which the information will be communicated, including the personal information protection principles applicable in that State.

This last factor may raise several questions since the ARPPIPS does not define what those "generally recognized principles regarding the protection of personal information" are.

However, the Québec privacy regulator, the Commission d'accès à l'information (CAI) published some guidance on this specific point, buried in its Guide on Conducting a Privacy Impact Assessment. The CAI remained cautious and indicated that it can be assumed that these "recognized principles" are general rules designed to ensure the protection of personal information, as well as the respect for the rights and interests of the persons concerned in this area [*our translation*]. The CAI also provided a non-exhaustive and non-definitive list of those principles inspired from (among others) the OECD Privacy Guidelines, the U.S. Federal Trade Commission's Fair Information Practice Principles (FIPPs), Canada's federal *Personal Information Protection and Electronic Documents Act*, and the European Union's *General Data Protection Regulation*.

In order to enhance their compliance with the assessment obligations set out in section 17 of the ARPPIPS, we recommend that organizations ensure that their PIA model allows for the evaluation of the following principles:

- **Accountability:** organizations are accountable for their management of personal information.
- **Identifying purposes:** the purposes for which personal information is collected are identified prior to collection.
- **Limiting collection:** organizations collect only the information necessary for the purposes identified. Information is collected by fair and lawful means.
- **Consent:** persons concerned are adequately informed of the identified purposes and freely consent to them unless an exception applies.
- **Protection by design and default:** products/services are designed with respect for the privacy of persons concerned. If they include privacy settings, these protect privacy by default.
- **Limiting use, disclosure and retention:** organizations use and disclose personal information collected for identified purposes or compatible purposes, except with consent or legal exception.
- **Accuracy:** organizations keep personal information up to date and ensure that it is accurate and complete at the time it is used or disclosed.

- **Security:** organizations take appropriate security measures to protect the information they hold at all times against loss, theft or unauthorized modification, disclosure or destruction.
- **Transparency:** organizations provide relevant information to data subjects at the time of collection or consent.
- **Data subject rights:** persons concerned can access their personal information and request rectification or, in certain cases, deletion.
- **Remedies:** in the event of dissatisfaction, people can contest a refusal to exercise a right or lodge a complaint with the organization or a competent body.

# Implementation of protective measures, including contractual measures

Section 17 of ARPPIPS 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 contractual safeguards 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 ARPPIPS requires that a written contract be entered into and that it:

- specifies the measures that the service provider must take to protect the confidentiality of the transferred personal information, 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;
- states 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
- states 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.

### Other recipients

Although the ARPPIPS 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 providers such as 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

While the *Personal Information Protection and Electronic Documents Act* (PIPEDA) does not explicitly require that organizations notify individuals that their personal information may be transferred outside of Canada, the Office of the Privacy Commissioner of Canada (OPC) published in 2009 its Guidelines for processing personal information across borders, in connection with 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.

The expected PIPEDA reform bill introduced by the federal government in June 2022 (Bill C-27) and currently under review by the Standing Committee on Industry and Technology, imposes, for the moment, an obligation of transparency with regard to international and interprovincial transfers. If adopted, as is, 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

Organizations should put in place the following measures to comply with the requirements of ARPPIPS with respect to transfers of personal information outside Québec:

- 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 model that allows for the analysis of the legal frameworks of the importing jurisdictions having regard to the generally recognized principles.
- Identify the jurisdictions where the organization will be transferring personal information. If their legal regime risks contravening the generally recognized 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 ARPPIPS requirements, having regard to the circumstances under which the transfers are to be made.

## Contact us

BLG's Cybersecurity, Privacy & Data Protection Group follows developments that could help businesses better understand the requirements in the ARPPIPS with regard to interprovincial and international transfers of personal information. Our team helps businesses implement the required compliance measures, including developing TIAs in compliance with applicable laws.

## Footnote

By

Candice Hévin, Catherine Labasi-Sammartino, Simon Du Perron

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