



Office of the
Privacy Commissioner
of Canada

PIPEDA

Processing Personal Data Across Borders **Guidelines**



PURPOSE

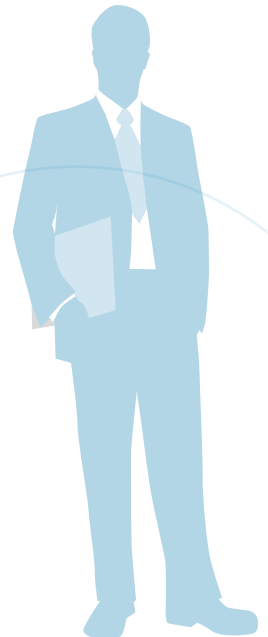
The Office of the Privacy Commissioner of Canada (OPC) has developed these guidelines to explain how the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to transfers of personal information to a third party, including a third party operating outside of Canada, for processing.


NOTE: The guidelines do not cover transfers of personal information for processing by federal, provincial or territorial public sector entities. Nor do these guidelines deal with any specific rules governing transfers for processing that may be found in provincial private sector privacy laws. However, organizations not governed by PIPEDA for commercial activities within a province need to be aware that PIPEDA applies to transborder transfers.

BACKGROUND

As the legislation itself states, PIPEDA is intended to “support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances...” This acknowledges that proper protection of personal information both facilitates and promotes commerce by building consumer confidence. Today’s globally interdependent economy relies on international flows of information. These cross-border transfers do raise some legitimate concerns about where personal information is going as well as what happens to it while in transit and after it arrives at some foreign destination. Consumer confidence will be enhanced, and trust will be fostered, if consumers know that transfers of their personal information are governed by clear and transparent rules.

There are different approaches to protecting personal information that is being transferred for processing. European Union member states have passed laws prohibiting the transfer of personal information to another jurisdiction unless the European Commission has determined that the other jurisdiction offers “adequate” protection for personal information.






In contrast to this state-to-state approach, Canada has, through PIPEDA, chosen an organization-to-organization approach that is not based on the concept of adequacy. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement. The OPC can investigate complaints and audit the personal information handling practices of organizations.

The key is Principle 1 of the CSA Model Code for the Protection of Personal Information, which forms Schedule 1 of PIPEDA. Principle 1 addresses the balance between the protection of personal information of individuals and the business necessity of transferring personal information for various reasons, including the availability of service providers, efficiency and economy.

Principle 1 places responsibility on an organization for protecting personal information under its control. Principle 4.1.3 of Schedule 1 of PIPEDA specifically recognizes that personal information may be transferred to third parties for processing. It also requires organizations to use contractual or other means to “provide a comparable level of protection while the information is being processed by the third party.”

Principle 1 states:



“An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.”

WHAT DO THESE TERMS IN PRINCIPLE 1 MEAN?

Transfer

“Transfer” is a use by the organization. It is not to be confused with a disclosure. When an organization transfers personal information for processing, it can only be used for the purposes for which the information was originally collected. A simple example is the transferring of personal information for the purpose of processing payments to customers. Or to use another example, an internet service provider may transfer personal information to a third party to ensure that technical support is available on a 24/7 basis. Increasingly, organizations outsource processes to third parties. In many cases, this involves the transfer of personal information. In the context of this document, when we refer to outsourcing, we are referring specifically to outsourcing that involves personal information.

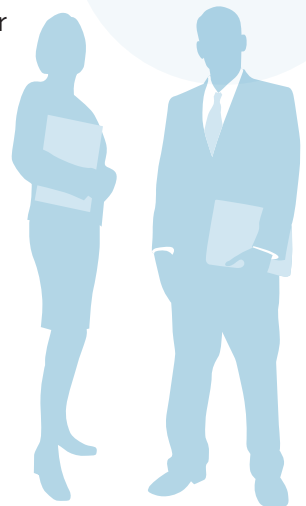
PIPEDA does not distinguish between domestic and international transfers of data.

Processing

“Processing” is interpreted to include any use of the information by the third party processor for a purpose for which the transferring organization can use it.

Comparable Level of Protection

“Comparable level of protection” means that the third party processor must provide protection that can be compared to the level of protection the personal information would receive if it had not been transferred. It does not mean that the protections must be the same across the board but it does mean that they should be generally equivalent.



WHAT MUST ORGANIZATIONS DO?

As the principle suggests, the primary means by which an organization may protect personal information that is sent to a third party for processing is through a contract.

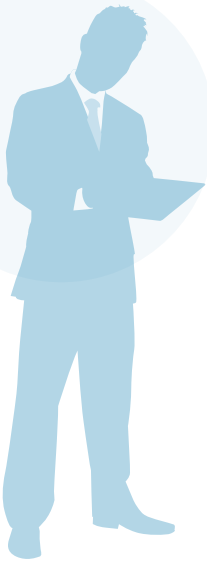
Regardless of where the information is being processed - whether in Canada or in a foreign country - the organization must take all reasonable steps to protect it from unauthorized uses and disclosures while it is in the hands of the third party processor. The organization must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times. It should also have the right to audit and inspect how the third party handles and stores personal information, and exercise the right to audit and inspect when warranted.

The OPC recognizes the complexity of the electronic world and understands that it is often impossible for an organization to know precisely where information is flowing while in transit. But that being said, the law is clear on where accountability lies and organizations must in their own best interests, as well as those of their customers, do what they can to protect the information.

What the organization cannot do through contract - or indeed by any other means - is to override the laws of a foreign jurisdiction.

So, what can an organization do to fulfill its obligations under Principle 4.1.3 of Schedule 1 of PIPEDA when it comes to transfers to foreign jurisdictions with respect to the issue of access to the personal information by foreign courts, law enforcement and national security authorities?

In an investigation into a complaint involving outsourcing to a U.S. firm by CIBC Visa, the OPC found CIBC to be in compliance with PIPEDA. The OPC relied on the Office of the



Superintendent of Financial Institutions' guidelines for federally regulated financial institutions. Those guidelines advise organizations to pay particular attention to the legal requirements of the jurisdiction in which the third party processor operates, as well the "potential foreign political, economic and social conditions, and events that may conspire to reduce the foreign service provider's ability to provide the service, as well as any additional risk factors that may require adjustment to the risk management program."

While these guidelines set a high standard for the protection of sensitive financial information by financial institutions, other organizations transferring sensitive personal information would also be well-advised to take note of them.

We assume that any organization looking at outsourcing to another jurisdiction will take a number of factors into account - for example, potential cost savings, the ability to provide better customer service, the availability of specialized expertise outside the company and other practical considerations.

In the case of outsourcing to another jurisdiction, PIPEDA *does not* require a measure by measure comparison by organizations of foreign laws with Canadian laws. But it *does* require organizations to take into consideration all of the elements surrounding the transaction. The result may well be that some transfers are unwise because of the uncertain nature of the foreign regime or that in some cases information is so sensitive that it should not be sent to any foreign jurisdiction.

Organizations need to be diligent in all their dealings with foreign third party processors.

Why Comply?

- Your customers expect you to be transparent about your practices: they will ask.
- These are best practices: following them may give you a competitive advantage.
- The law requires you to protect personal information while it is in the hands of a third party processor: failure to comply could result in complaints and legal action.



WHAT SHOULD INDIVIDUALS EXPECT?

Individuals should expect that their personal information is protected, regardless of where it's processed. Organizations transferring personal information to third parties are ultimately responsible for safeguarding that information. Individuals should expect transparency on the part of organizations when it comes to transferring to foreign jurisdictions.

Individuals have the right to assess their own risks when it comes to potential access to their personal information by foreign authorities. Some people are more risk averse than others. Some are willing to take a degree of risk in return for convenience or for access to a particular service.

Organizations need to **make it plain** to individuals that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction. They must do this in **clear and understandable** language. Ideally they should do it **at the time the information is collected**. Once an informed individual has chosen to do business with a particular company, they do not have an additional right to refuse to have their information transferred.

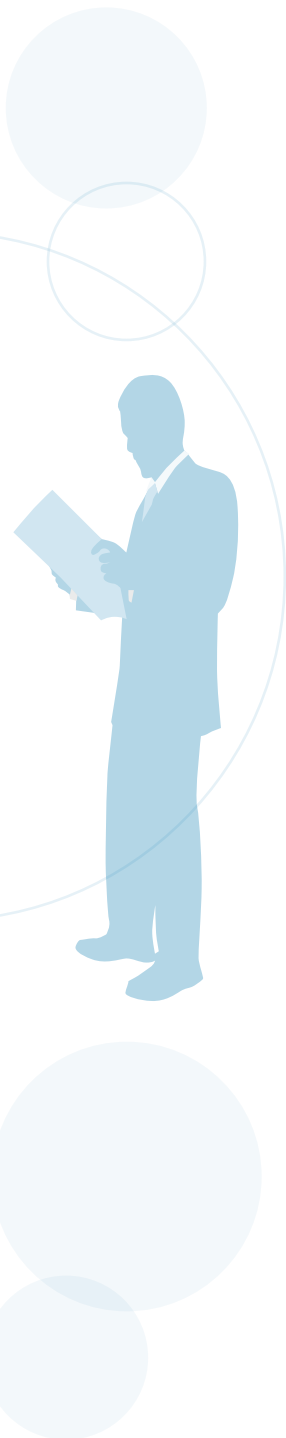
Tips for Individuals

- Expect transparency from organizations: but if in doubt ask
- Recognize that transborder flows of information are a fact of life and are very common
- Be a privacy wise consumer: don't assume that because you have "nothing to hide" you shouldn't do everything you can to exert control over information about you
- If you are uncomfortable, you may want to check out the privacy practices of other organizations. You can also discuss your concerns with our Office

SUMMARY OF KEY FINDINGS

The OPC has made a number of findings related to cross-border transfers of personal information in its complaint investigations over the past several years:

- PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing.
- PIPEDA does establish rules governing transfers for processing.
- A transfer for processing is a “use” of the information; it is not a disclosure. Assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required.
- The transferring organization is accountable for the information in the hands of the organization to which it has been transferred.
- Organizations must protect the personal information in the hands of processors. The primary means by which this is accomplished is through contract.
- No contract can override the criminal, national security or any other laws of the country to which the information has been transferred.
- It is important for organizations to assess the risks that could jeopardize the integrity, security and confidentiality of customer personal information when it is transferred to third-party service providers operating outside of Canada.
- Organizations must be transparent about their personal information handling practices. This includes advising customers that their personal information may be sent to another jurisdiction for processing and that while the information is in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities.





Office of the
Privacy Commissioner
of Canada

FOR MORE INFORMATION

The OPC has issued a number of investigative findings related to cross-border transfers of personal information. In all of these cases we have found that the transfer did not violate PIPEDA. See the following PIPEDA case summaries on the OPC web site, www.privcom.gc.ca:

- #394: Outsourcing of Canada.com e-mail services to U.S.-based firm raises questions for subscribers
- #365: Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered
- #313: Bank's notification to customers triggers *PATRIOT Act* concerns

Industry Canada has additional material on its web site. Visit: <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00508.html>