

TIMI OLAOYE
January 19th, 2024

(PIPEDA) Personal Information Protection and Electronic Documents Act:

EXPLORING THE TENETS OF THE CANADIAN PRIVACY SPACE



Introduction

With the rise of the "Dot-Com Bubble" from the late 1990s and early 2000s, there was an upward trend in the emergence of online commercial enterprises around the globe. Subsequently, the impetus for ensuring the protection of personal information within the

digital commercial space arose, which led to several privacy laws and regulations enacted around the globe by various governments and institutions.

On January 1st, 2001, the Canadian parliament enacted the **Personal Information Protection and Electronic Documents Act**, also known as **PIPEDA**.

PIPEDA sets out guided stipulations to aid commercial institutions on how to collect, use, and disclose personal information, additionally grants individuals “power over their personal information” via access, rights, consent, and a few other guard rails to ensure individuals can dictate the utility of their personal information.

The Office of the Privacy Commissioner (OPC) enforces and monitors organizations to validate compliance with the PIPEDA stipulations. This includes probing reported complaints from individuals in cases where organizations may have violated their privacy rights.

Personal Information

The Ontario Privacy Commissioner defines Personal information, also known as "PI" under PIPEDA, as " any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- Age, name, ID numbers, income, ethnic origin, or blood type.
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, the existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)"

What are the PIPEDA Principles?

Principles are simply rules that direct or govern a decision-making system. The PIPEDA informational principles are no different. They offer ten rules/tenets that aid organizations in accumulating, utilizing, and disseminating an individual's personal information. These

principles provide a foundational approach organizations must abide by to ensure duty of care from a personal information perspective.

The PIPEDA Informational Principles are as follows:

- **Accountability** - Accountability ensures that organizations own individuals' personal information. It requires organizations to deploy duty of care measures by assigning individuals or teams to ensure alignment with PIPEDA requirements.
- **Purpose Identification** - Organizations must have a "raison d'être" when collecting personal information, at or before collection. The question is, for what purpose is the PI collected as understood by the individual providing the information?
- **Consent** - Consent involves providing details on 'specific information being collected,' 'reason for information collection,' and how that information will be used or disclosed,' stated in simple and plain language, and the individual, after having understood the reason for collection voluntarily providing permission or agreeing to that purpose. Organizations should ensure consent is provided before or during PI collection.
- **Collection Limitations** - Once the details around the specificity of the Personal Information collected have been disclosed and consented to, organizations are prohibited from collecting beyond the stipulated agreement.
- **Limiting Use, Disclosure, and Retention** - In addition to restricting the use and disclosure of personal information within the stipulated purpose of the collection agreement between the individual and the organization, there is also a requirement to ensure information is retained only within the specified time or retention period.
(Visit my article on [Enterprise Data Lifecycle Management](#) to learn more about Enterprise data retention)
- **Accuracy** - Organizations must continually ensure the accuracy, completeness, and validity of personal information to fulfill the intended purpose of use.
- **Safeguards** - Proportional guardrails about the sensitivity of personal information collected should be set in place by organizations to ensure adequate security.

-
- **Openness** - Organizations must explicitly set out their policies and procedures for handling personal information, ensuring transparency and integrity.
 - **Individual Access** - Upon request by an individual, organizations must provide individuals with details surrounding the existence, utilization, and dissemination of their personal information within a reasonable time. Under PIPEDA, individuals also retain the right to challenge the accuracy and completeness of their data, allowing modifications upon request by the individual as appropriate.
 - **Challenging Compliance** - Individuals uphold the prerogative of challenging organizations that fail to ensure alignment with the PIPEDA principles concerning individuals. Organizations must provide a 'designated individual' to ensure compliance with PIPEDA, which in most cases falls under the authority of the company's "Chief Privacy Officer."

PIPEDA Circumstantial Exceptions

As with most regulations, the principles of fairness and reasonableness are considered. Here are a few circumstances whereby PIPEDA regulations do not apply as follows:

- **Non-profit and Political Organizations** - Non-profit and political organizations do not fall under the scope of PIPEDA, except those engaged in commercial activity as their primary directive and or utilize personal information for such purposes.
- **Personal Purposes (i.e., Holiday greeting card lists)**
- **Federal government bodies stipulated within the Privacy Act**
- **Provincial and territorial governments (including their agents)**

Sources

[Office of the Privacy Commissioner OPC](#)

[Investopedia](#)

