Your Guide to PIPEDA

Author : Cat

Date : December 24, 2020

What is PIPEDA?

The *Personal Information and Electronic Documents Act* is a framework of legal guidelines for collection and processing of personal info of individuals within Canada. Or, in short, it's a set of rules that companies need to follow to collect and protect a user's data. PIPEDA applies to any private-sector organization within Canada as well as international companies that collect and process Canadian data. Public sector, or government agencies, fall under the Canadian Privacy Act.

Some provinces, including British Columbia, Alberta, and Quebec, have provincial laws that are

considered "substantially similar" and supersede PIPEDA in those provinces. Additionally, Canada has various provincial medical data regulations, above PIPEDA if you deal with Personal Health Data.

Terms to understand:

Personal Information – any identifying information . This includes submitted information such as your name, email, SIN, address, phone number, biometrics, or account numbers. It also includes information that could be used to identify you indirectly such as location data.

Personal Health Information – Any personal information having to do with health or residing within a health record.

Fair Information Principles

PIPEDA is guided by 10 fair information principles. These principles define how data is collected, used, stored, transferred, and retained. They also define how this has to be communicated to the individuals involved.

Below is a brief definition of each Principle and a link to the government page that provides an expanded explanation.

Principle	Definition
Accountability	The organization is responsible for the data under its control.
Identifying Purposes	The purpose for collecting the data must be made clear
Consent	The organization must obtain consent to collect,

	use or disclose data.
Limiting Collection	Data collection shall be limited to only what is necessary.
Limiting Use, Disclosure, & Retention	Data use, disclosure and retention must be limited to the purpose for which it was collected, except by law.
Accuracy	Personal Information must be accurate, complete, and up-to-date.
Safeguards	The organization must employ appropriate safeguards in line with the sensitivity of the data.
Openness	The privacy policies and practices of the organization must be readily available and accessible.
Individual Access	An individual shall be able to access to the data retained and permitted to challenge accuracy.
Challenging Compliance	An individual must be able to address concerns of compliance with the designated individual(s) accountable for their data.

A few highlights from the regulation:

Individual Access – As a Canadian Citizen, you have the right to access your data held by a company. You also have the right to ask for that data to be updated if it is inaccurate.

Consent – For all data collection, the individual has to have the ability to both opt in AND withdraw consent. Companies also have to present the information in a clear way. I like to break these down as the 5 Ws:

- WHO – Details of the recipients of the data
- WHAT – List of the data being collected
- WHY – Reason for the collection (*known as legal basis*)
- WHEN – The duration for which the data will be retained
- WHERE – Clear links provided so user knows where to go to enact requests

The simplest way to satisfy this right is to put all the information in your *Privacy Policy.*

Privacy Incident Management and Breaches – In terms of protection of data, this is a big one. In the past there was NO regulation that a company had to report a privacy breach. Uber took 6 months to report their 2018 data breach. Under PIPEDA, companies must report any breach that represents a significant risk of harm to the individual. Breaches can be reported directly via the government breach site.

For Businesses and Corporations

Any organization that is Canadian or serves Canadian citizens must comply under PIPEDA. It is recommended that you assign an individual in your company who is responsible for the implementation of you privacy program and overseeing of compliance.

If your company handles sensitive data and/or health data, you shoud run a **PIA,** or *Privacy Impact Assessment,* that includes an explanation why you are collecting the data requested, an assessment of risks to the rights and freedoms of data subjects, and documented proposed measures for safety and security of the collection.

Global Privacy Regulation Compliance is largely what WE do as a company. From DIY checklists to templates to having us do it for you, contact us for more information on how we can help.

Bill C-11

In late 2020, a new amendment was proposed to PIPEDA called Bill C-11. The new regulation is currently being called CPPA or the *Consumer Privacy Protection Act*. There are many improvements in the new bill including:

- Right to deletion of an individual's data from the system
- Hefty fines for non-compliance
- Requirement for a Privacy Program and policies
- Better technical definitions around terms such as de-identification

Look for this bill to become law in late 2021 or early 2022.

More Help and Information

For full details on PIPEDA in Canada, visit the government PIPEDA page.

An overview of CPPA (or Bill C-11) can be found via the IAPP (International Accusation of Privacy Professionals).

If you want help from our consultants, have any questions or find something we've missed let us know!