SPOTLIGHT ON CANADA'S PRIVACY LAWS

Regulatory Requirements and Principles Under the Privacy Laws in Canada

A Spotlight on the Main Federal Laws for the Collection, Use and Disclosure of Personal Information in Canada

StratisAdvisory

RISK | STRATEGY | CYBER | COMPLIANCE MANAGEMENT

Privacy Laws in Canada

There are a number of laws covering privacy rights in Canada, depending on the type and location of an organization, as well as the type and the reach of information. However, there are two (2) main federal privacy laws in Canada dealing with personal information, the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA), both enforced by the Office of the Privacy Commissioner of Canada.

PRIVACY ACT		PIPEDA
Personal information is defined as "any recorded information about an identifiable individual," including but not limited to nationality, religion, age, marital status, individual historical records, address, fingerprints, blood type, personal opinions or views, or the name of the individual where it appears with other personal information.	**Definition**	Personal information is defined as "any factual or subjective information, recorded or not, about an identifiable individual," including but not limited to name, age, income, ethnicity, social status, blood type, opinions, evaluations, disputes, disciplinary actions, employee files, credit/loan records, medical records, or intentions.
Collection, use, disclosure, retention or disposal of personal information in the course of providing government services.	**Type of Activity**	Collection, use, or disclosure of personal information in the course of commercial activity.
Applicable to Crown corporations and to federal government institutions listed in Schedule/Section 3 of the Privacy Act.	**Applicability**	Applicable to private sector organizations, as well as federally regulated organizations, organizations in certain territories that are considered federally regulated, and commercial businesses that operate across provincial and national borders.
Political parties, political representatives such as senators or parliament members, courts and private sector organizations.	**Exemptions**	Charity and not-for-profit groups unless engaged in commercial activities as their core, political parties, municipalities, universities, schools and hospitals. and certain personal information covered by the Privacy Act or those used for business communication, personal, journalistic, artistic or literary purposes.

Office of the Privacy Commissioner of Canada

IMPORTANT:

Each province and territory have laws that govern their public sectors, which can be found here.

The Privacy Act

The goal of the Privacy Act R.S.C, 1985 (the Act) is to safeguard and defend an individual's privacy and personal information at the disposal by a government institution. It is the law that sets out privacy rights of Canadians in relation to how personal information is collected, used and disclosed through federal government interactions and also allows them the right to have access to that information. Below are the requirements for handling personal information:

Denying Access

The federal or government institution may deny access to personal information if disclosure is:

- *Harmful to Canada's federal, provincial or international affairs' defence;*
- *Subject to solicitor-client privilege or related to information obtained by an investigative body;*
- *A safety threat or is related to physical or mental health.*

Right to Access

Access to personal information may be requested in writing from the federal institution that holds it.

Disclosure

No disclosure without consent and alignment to purpose unless:

- *Authorized in federal legislation;*
- *It complies with subpoenas; or*
- *Personal and public interest transcends invasion of privacy.*

Collection

Personal information can only be collected if with consent and if related to program operation or activities.

Use

Personal information must only be used for specified or identified purpose.

Accuracy

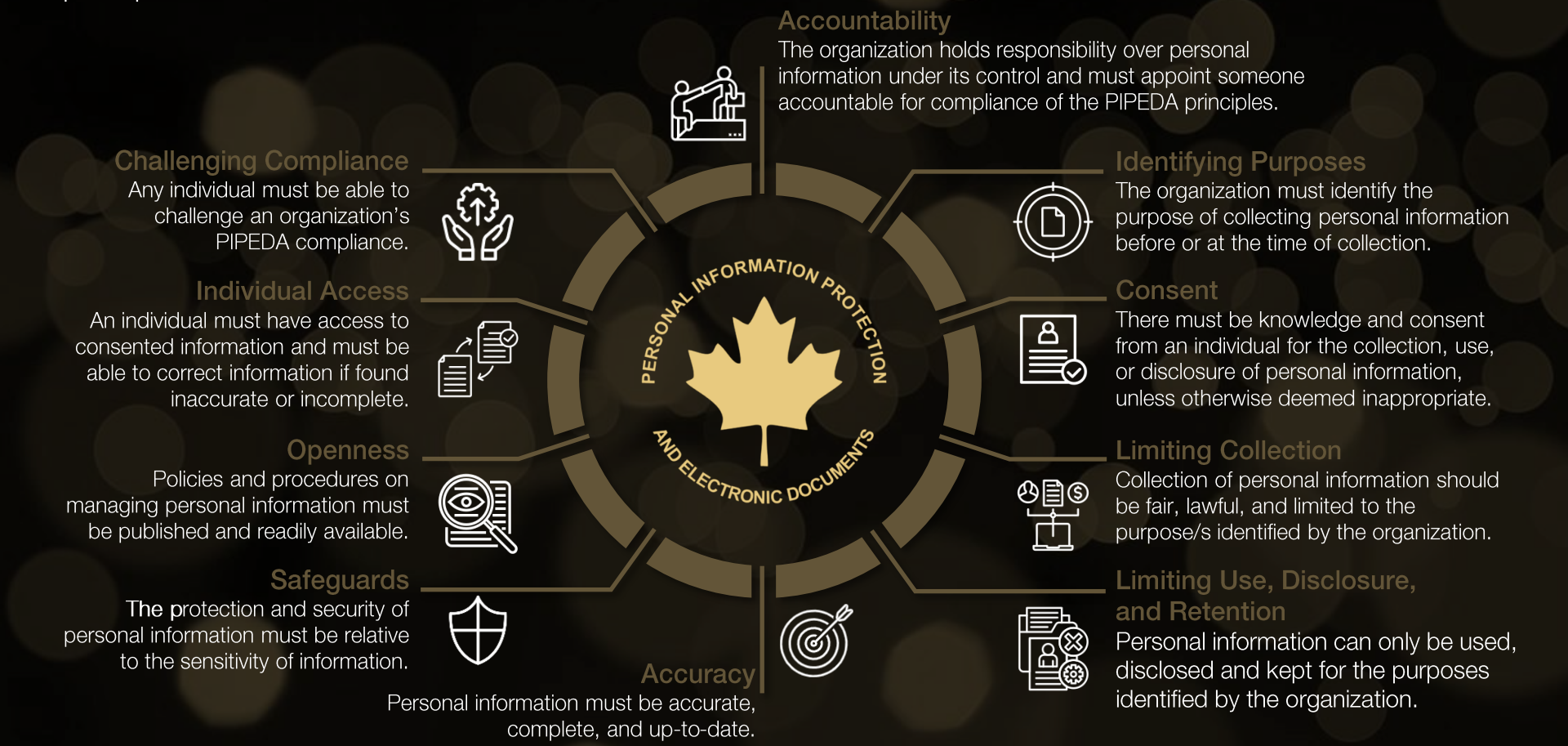
Must ensure that personal information is accurate, up-to-date and complete.

Retention

Personal information is retained for 2 years or if disposal consent is given.

The PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA), on the other hand, is the federal law that governs how private sector organizations collect, use and disclose personal information during the course of commercial activity. Moreover, PIPEDA is also applicable to federally regulated organizations when it comes to their employees' personal information. Below are the ten (10) fair information principles under the PIPEDA:



Accountability
The organization holds responsibility over personal information under its control and must appoint someone accountable for compliance of the PIPEDA principles.

Identifying Purposes
The organization must identify the purpose of collecting personal information before or at the time of collection.

Consent
There must be knowledge and consent from an individual for the collection, use, or disclosure of personal information, unless otherwise deemed inappropriate.

Limiting Collection
Collection of personal information should be fair, lawful, and limited to the purpose/s identified by the organization.

Limiting Use, Disclosure, and Retention
Personal information can only be used, disclosed and kept for the purposes identified by the organization.

Accuracy
Personal information must be accurate, complete, and up-to-date.

Safeguards
The protection and security of personal information must be relative to the sensitivity of information.

Openness
Policies and procedures on managing personal information must be published and readily available.

Individual Access
An individual must have access to consented information and must be able to correct information if found inaccurate or incomplete.

Challenging Compliance
Any individual must be able to challenge an organization's PIPEDA compliance.

Discover what Stratis Advisory can do for you

Privacy Risk Assessment

From collecting basic platform usable information on a user to collecting customer information such as personally identifiable information (PII), how you collect, gather, store, transfer, and use such data is critical to maintaining compliance with various global privacy laws. Stratis can assess your current and future data gathering practices as you open new markets, acquire companies, and launch new products that require different customer disclosures.

Customer Experience Data Analysis

From the earliest interactions with a user to collecting PII, customer interactions leave behind a data trail that can be leveraged for marketing, security, and enhanced customer experiences. Stratis can help you evaluate existing onboarding and due diligence processes to ensure your data gathering meets regulatory requirements, appropriate disclosures, and data retention requirements as a data controller or processor.

Outsourced Regulatory Monitoring Program

Operating domestically or globally, industry guidance and laws and regulations are evolving and expanding, specifically those on beneficial ownership reporting, data privacy and breach reporting, cybersecurity program implementation, and third-party risk management. Stratis can develop and execute a customized outsourced regulatory monitoring program based on your operating model, markets, customers, and risk tolerance to proactively address relevant changes that impact your business.

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com