whitepaper

CANADA'S PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

Canada's federal private sector data privacy law

In 2001, the Office of the Privacy Commissioner of Canada ("OPC") created a federal act titled Personal Information Protection and Electronic Documents Act ("PIPEDA"), that regulates the way private-sector organizations "collect, use, and disclose personal information in the course of for-profit commercial activities across Canada." PIPEDA was last amended on June 23, 2015 and this is the current version used by the OPC.

The OPC recently issued two documents to reinforce PIPEDA requirements and standard expectations. These documents are titled: 1) Guidance on Inappropriate data practices: Interpretation and application of subsection 5(3); and 2) Guidelines for Obtaining Meaningful Consent.

The OPC will begin to apply "Guidance on Inappropriate data practices" on **July 1, 2018**, however, organizations are not expected to comply with "Guidelines for Obtaining Meaningful Consent" until **January 1, 2019**.

Below is a summary of PIPEDA, which includes the OPC's newly issued guidance.

PIPEDA COMPONENTS

PIPEDA is divided into two main parts, separating requirements 1) for personal data and 2) for electronic documents, with an additional addendum that sets a National Standard for data protection titled "Schedule 1." Part I is titled "Protections of Personal Information in the Private Sector" and consists of five divisions addressing the following: the protection of personal information, remedies, compliance agreements, audits, general matters, and transitional provisions. Part 2 is titled "Electronic Documents" and addresses the following: electronic alternatives to paper records, regulations, and orders.

Schedule 1 provides standards for organizations to comply with privacy requirements under PIPEDA. Schedule 1 consists of ten principles that address an organization's obligations related to the following: 1) Accountability; 2) Purpose; 3) Consent; 4) Limits on collection; 5) Limits on use, disclosure, and retention; 6) Accuracy; 7) Safeguards; 8) Openness; 9) Individual Access; and 10) Challenging Compliance.

COVERED INFORMATION AND APPLICABLE ORGANIZATIONS

PIPEDA covers all personal information, defined as any information about an identifiable individual. This may include age, name, ID numbers, income, or employee files.

PIPEDA applies to "every organization in respect of personal information" that either collects, uses, or discloses personal information in the course of commercial activities OR in connection with the operation of a "federal work, undertaking, or business" (FWUB)[1]. An organization is broadly defined as any "association, partnership, person or trade union." Additionally, an organization is responsible for "personal information in its possession or custody, including information that has been transferred to a third party for processing."

An organization is required to comply in the course of **commercial activities** when the organization discloses personal information during an international transaction, act, conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund-raising lists. This includes organizations that engage in commercial activities involving inter-provincial or international personal information flows as well as import and export businesses. Additionally, the OPC states that although most provinces have separate laws that apply to credit reporting agencies, credit bureaus must comply with PIPEDA with respect to cross-border personal information collection, use, or disclosure.[2]

An organization may be required to comply as an **FWUB** if the organization discloses personal information in connection with work, undertaking, or business that is under the legislative authority of Parliament. Examples of FWUB might include work connecting provinces, air transportation, radio broadcasting, or anything defined in the Bank Act or Oceans Act.[3]

EXCLUDED ORGANIZATIONS FROM PIPEDA

Government institutions under the Privacy Act do not need to comply with PIPEDA, along with facilities that use an individual's business contact information in relation to the individual's employment, business, or profession. Additionally, individuals who collect, use, or disclose data for either personal or domestic purposes or journalistic,

1 Office of the Privacy Commissioner of Canada, Section on PIPEDA in Brief, What is a "FWUB," https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/
2 Id.
3 Id.

literary or artistic purposes are not subject to comply with PIPEDA. Finally, PIPEDA does not apply to (1) not-for-profit and charity groups or (2) political parties and associations.[4]

PROCEDURES

Schedule 1 implements requirements for any organization that collects, uses, or discloses personal information. These requirements fall under ten separate "principles."

1) Accountability

Organizations must designate an individual, separate from "other individuals within the organization [who] may be responsible for day-to-day collection and processing."[5] Additionally, the individual's identity should be made available upon request. Organizations must implement policies to give effect to PIPEDA principles, including:

- Procedures to protect personal information;
- Procedures to receive and respond to complaints and inquiries ;
- Training for staff on applicable policies;
- Information that explains the organization's policies.

2) Purpose

Organizations must state an appropriate purpose to "collect, use or disclose personal information" that a "reasonable person" would consider appropriate. If a "certificate under section 38.13 of the Canada Evidence Act" prohibits disclosure or the organization is a business with the primary purpose of purchasing or selling personal information, the organization may not disclose the individual's personal information without consent.[6]

3) Consent

The OPC does not give a prescribed consent form to follow but expects companies to develop a consent process that meets regulatory obligations. **This section covers the information addressed in the OPC's newly issued "Guidance on Obtaining Meaningful Consent."**

---

4 Id.
5 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Schedule 1.
6 Id.

a. Consent Exemptions

Several circumstances exist where an organization is not required to obtain consent from an individual before collecting, using, or disclosing personal information.

PIPEDA permits organizations to ***collect*** information without consent when:

- collection is in the interest of the individual and cannot be obtained in a timely way;
- collection is reasonable for purposes of investigating a breach and consent would compromise the availability or accuracy of the information;
- collection of information is for journalistic purposes; or
- the organization is collecting publically available information.[7]

PIPEDA permits organizations to ***use*** information without consent when:

- the organization becomes aware that information could "be useful in the investigation of a contravention of the laws of Canada" and used for the purposes of investigating;
- the organization responds to an emergency threatening "the life, health or security of an individual";
- the organization uses publically available information or statistic information from scholarly research where it is impractical to obtain consent.[8]

7 Id. at Division 1, Section 7.4.
8 Id.

PIPEDA permits organizations to ***disclose*** information without consent when:

- the information is disclosed to a notary in Quebec;
- the organization is collecting debt owed by the individual;
- the organization discloses information under court orders or requirements to comply with subpoena;
- the organization discloses information in the interest of national security;
- the organization disclosed the information for the reasonable purpose of detecting, preventing, or suppressing fraud.

PIPEDA refers to more instances where organizations do not need to obtain consent in Section 7. Section 7.2 also limits an organization's requirement to obtain consent with respect to prospective business transactions and completed business transactions.[9]

b. Requirements for Consent

Firstly, organizations must make four key elements readily available within a consent form in order for individuals to understand the nature, purpose, and consequences of what is being consented to. These key elements are as follows:[10]

(1) The organization must specify **what personal information will be collected** from the individual.

(2) The organization must disclose **which parties will be receiving** this information. PIPEDA expects the organization to clearly specify which third parties will receive the individual's information and express if the third party will use information for their own purpose.

9 Id.

10 Office of the Privacy Commissioner of Canada, Guidelines on Meaningful Consent, Emphasize Key Elements, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/#fn12.

(3) The organization must clearly state its **purpose for collecting** an individual's personal information. At a bare minimum, the organization should inform the individual of its purpose using "sufficient detail" without vague terms and highlighting what is not obvious.

(4) The organization must emphasize the **risk of harm** and other consequences. Consent is valid if the individual can reasonably foresee a potential risk and understands the consequences of consent. If a consequence involves a potential meaningful risk, the organization must notify the individual. Meaningful risks are more than a minimal or mere possibility and include bodily harm, financial loss, identity theft, or negative effects on an individual's credit record.

Secondly, PIPEDA requires organizations to increase the role of individuals in the consent process. Individuals must be able to easily access information and control "how much detail they wish to obtain, and when." PIPEDA recommends for organizations to implement a "multilayered privacy notice"[11] allowing individuals to review information he or she already consented to and verify the terms of the agreement without feeling compelled to consent. Individuals must be able to reconsider consent at any time with a clear "opt-in" or "opt-out" option available. The OPC suggests for organizations to innovate their consent forms, making them mobile or online, and to use pilot testing to ensure consent form language is actually user-friendly. If an organization requires consent for a condition of service, the individual's private information must be integral to the service and required for a legitimate purpose. PIPEDA requires an organization requesting information from anyone under the age of 13 to obtain consent from a parent or guardian. [12]

Generally, under PIPEDA, organizations must ensure they have an appropriate purpose for collecting, using, or disclosing personal data that is defined and that a reasonable person would find appropriate. An individual's consent to collect data for one purpose does not give the organization unlimited authority to use or collect the individual's information for any purpose; the organization must obtain additional consent for any separate purpose not previously mentioned to the individual.

The Supreme Court of Canada outlined three instances where an organization must obtain **express consent** from an individual, even if the individual already gave general consent.[13] The first instance is when the organization is

11 Hunton & Williams LLP, Ten Steps to Develop a Multilayered Privacy Notice, The Center for Information Policy Leadership, https://www.hunton.com/files/Publication/37a71d77-14c4-4361-a62b-89f67feb544f/Presentation/PublicationAttachment/e7ffca9d-da66-4ed6-a445-f8fdc0b97e22/Ten_Steps_whitepaper.pdf.
12 Office of the Privacy Commissioner of Canada, Guidelines on Meaningful Consent, Allow individuals to Control, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/#fn12.
13 Royal Bank of Canada v. Trang, 2016 SCC 50 § 23. See also Alberta PIPA, sections 8(2) – 8(2.2), 8(4).

requesting sensitive information from the individual, relating to the individual's health or financial status. The second instance is when the organization is collecting the individual's information for a purpose outside of a consumer's reasonable expectations. This may include tracking the individual or allowing third-party access to the individual's information. The final instance is the organization may create a significant harm by collecting or using the individual's personal data.

4) Collection

The amount and type of personal information collected must be limited to "that which is necessary" for the organization's identified purpose. PIPEDA requires organizations to specify the type of information collected, as set forth in "Openness" principles.

5) Use, Disclosure, Retention

Organizations must implement "minimum and maximum retention periods" for holding an individual's personal data. The organization must retain personal information "long enough to allow the individual access to the information after the decision has been made." Personal information must be "destroyed, erased, or made anonymous" when the information is no longer required to fulfill its identified purpose.[14]

6) Accuracy

PIPEDA requires that personal information be as "accurate, complete, and up-to-date" as necessary for its specified purpose. At all times, personal information should at least be accurate, complete, and up- to-date to "minimize the possibility that inappropriate information may be used to make a decision about an individual."

Personal information "used on an ongoing basis, including information that is disclosed to third parties" should be accurate and up-to-date, unless accuracy requirements are "clearly set out." Otherwise, organizations "shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected."[15]

7) Safeguards

Organizations must adopt security measures to protect sensitive personal information against "loss or theft, as well as unauthorized access, disclosure, copying, use, or modification."

Measures must include:

- Educating employees on the importance of maintaining confidentiality;
- Physical measures, such as locked filing cabinets and restricted access to officers;
- Organizational measures, such as security clearances and limited access on a "need-to-know" basis; and
- Technological measures, such as the use of passwords and encryption.[16]

14 Id.
15 Id.
16 Id.

8) Openness

Individuals must be able to access an organization's policies "without unreasonable effort." An organization's policies must include information that addresses:

- The name or title, and the address, of the person accountable for the organization's policies and practices and to whom complaints and inquiries can be forwarded;
- The means of gaining access to personal information held by the organization;
- A description of the type of personal information held by the organization, including a general account of its use;
- A copy of any brochures or other information that explain the organization's policies, standards, or codes; and
- What personal information is made available to related organizations (e.g., subsidiaries).[17]

9) Individual Access

Organizations must inform an individual of the "existence, use, and disclosure of his or her personal information and shall be given access to that information," upon the individual's request. This includes information disclosed to a governmental institution for a subpoena, warrant, or other government request. Organizations must respond to an individual's request in a timely manner, and if the organization cannot accommodate the individual's request, the organization must give "reasons for denying access" to the personal information.

An organization may only refuse access to personal information if: (a) the information is protected by solicitor-client privilege or, in civil law, by the professional secrecy of lawyers and notaries; (b) to do so would reveal confidential commercial information; (c) to do so could reasonably be expected to threaten the life or security of another individual; (d) the information was generated in the course of a formal dispute resolution process; or (e) the information was created for the purpose of making a disclosure under the Public Servants Disclosure Protection Act or in the course of an investigation into a disclosure under that Act.[18]

17 Id.
18 Id.

10) Challenging Compliance

An individual has the right to file a written complaint with the Commissioner if he believes an organization is not following a provisions or recommendation stated above. The Commissioner will investigate all complaints unless (1) there are other resources for the individual to exhaust, (2) the complaint could be dealt with initially or completely by procedures under other laws, or (3) the complaint was not filed within a reasonable number of days. The Commissioner is also not required to investigate a complaint if he believes an investigation would contravene sec. 6-9 stated under "Remedies." The Commissioner may discontinue an investigation or reconsider an investigation if the individual shows a compelling reason.[19]

After an investigation, PIPEDA requires that the Commissioner send out a prepared report with findings and recommendations to the individual and the organization. This report may require an organization to correct its practices, publish a notice of action, or award damages to the individual, also referred to as the "complainant." Organization are liable for failing to comply with terms and policy requirements issued by the Commissioner. The Commissioner may also audit an organization if there are reasonable grounds to believe the organization is not following a recommendation in Schedule 1 or a provision above.

ELECTRONIC ALTERNATIVES

PIPEDA allows for the use of electronic means to "create, collect, receive, store, transfer, dispute, publish or otherwise deal with documents" when federal law does not require otherwise. Data retention requirements by federal law are satisfied if (a) the electronic document is retained for the specified period in the format in which it was made, sent or received, or in a format that does not change the information contained in the electronic document that was originally made, sent or received; (b) the information in the electronic document will be readable or perceivable by any person who is entitled to have access to the electronic document or who is authorized to require the production of the electronic document; and (c) if the electronic document was sent or received, any information that identifies the origin and destination of the electronic document and the date and time when it was sent or received is also retained.

RESTRICTED PRACTICES AND NO-GO ZONES[20]

As previously mentioned, the OPC issued Subsection 5(3), which implements boundaries where organization cannot venture for data, also known as "No-go Zones." Subsection 5(3) reads: "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." Courts enforce that an organization's "purpose" must be viewed from a reasonable person's perspective and read in light of the entire act to properly balance an individual's privacy with an organization's interest for personal data. Subsection 5(3) creates an overarching standard for organizations to follow when determining the "purpose" for personal data, but limits the organization to at least consider what a reasonable person would find appropriate with respect to the company's purpose for collection, use or disclosure of personal data.

The Canadian Federal Court of Appeals determined several factors to assess whether an organization's purpose for collecting, using, or disclosing person data is reasonable and complies with subsection 5(3). The factors are as follows:

19 *Id. at Division 2, Section 11-12.*
20 *Office of the Privacy Commissioner of Canada, Inappropriate Data Practices, No Go Zones, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/.*

1. The degree of sensitivity of the personal information at issue;
2. Whether the organization's purpose represents a legitimate need/bona fide business interest;
3. Whether the collection, use, and disclosure would be effective in meeting the organization's need;
4. Whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and
5. Whether the loss of privacy is proportional to the benefits

A No-Go Zone is a purpose for collection, use or disclosure of personal data that is generally considered inappropriate by a reasonable person. The established No-Go Zones include:

- Collecting or using personal data for an unlawful purpose;
- Profiling to allow for inferences about an individual or group;
- Collecting or using personal data that will harm an individual, which includes financial loss or identity theft;
- Charging an individual to remove published personal information; requiring passwords to access an individual's personal accounts; and
- Tracking an individual through audio or video.

In light of the above, organizations that conduct background screening on Canadian applicants and employees would be well advised to review such policies and practices with counsel, and to revise accordingly, to ensure compliance with PIPEDA (specifically, with any applicable disclosure and consent requirements). ■