Privacy Program Development

A No-Nonsense Guide to PIPEDA Compliance

TRUE NORTH

• PSR

Table of Contents

1.0 Introduction

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a key piece of Canadian federal privacy legislation which became law in April 2000.

1.1 To Whom Does PIPEDA Apply?

PIPEDA applies to private-sector organisations across Canada that process 'Personal Information' while doing business. In other words, if you collect, use, process, share, or store Personal Information in the course of running any commercial activities, then you're subject to PIPEDA or a "substantially similar" provincial privacy law.[1]

Check to find out whether the jurisdiction in which your company operates is impacted by one of those provincial laws.[2]

1.2 What's Personal Information?

This law regulates the use of Personal Information in commercial activity by private-sector organisations and outlines several key requirements for compliance.

'Personal Information' includes *"any factual or subjective information, recorded or not, about an identifiable individual."* That can be a lot of different things, but some common examples include:

- Contact information (e.g., address, email)
- Immutable characteristics (e.g., ethnicity, gender, blood type)
- Government records (e.g., passport number)
- Health information (e.g., medical conditions)
- Financial information (e.g., credit record)
- Personal beliefs (e.g., religious beliefs)

2.0 How Do I Comply With PIPEDA?

2.1 What is PIPEDA compliance?

PIPEDA compliance means fulfiling your company's obligations in accordance with the law's provisions and having the technical and operational controls in place.

As with any privacy law, compliance with PIPEDA is not a one-time exercise, nor can it be achieved through tick-box exercises. PIPEDA compliance is ongoing, and certain areas of the law, such as privacy rights requests and breach response, need continued attention.

---

[1] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/
[2] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/

2.2 Understanding your data

Developing a central data map is vital for your company's compliance program, improving your understanding of your data inventories (i.e., what data you have, how much data you have, where that data is) and the applicable laws to which your company is subject.

Further, understanding PIPEDA's definition of Personal Information (refer to the 'Introduction' section above) can help you to apply the correct regulatory context to the information your company has and ensure that requirements such as information provision requirements or privacy rights requests are met correctly.

Your company can also use an up-to-date data map to ensure processing activities comply with the ten Fair Information Principles that organisations are required to meet.

2.3 PIPEDA's 10 Fair Information Principles (FIPs)

Processing Personal Information in accordance with the ten Fair Information Principles (FIPs) set out by PIPEDA is essential for your company's compliance. The OPC describes the ten FIPs as the "ground rules" for processing and, if your company is subject to PIPEDA, you have to ensure those principles are met.

The ten Fair Information Principles[3] detailed within the law are:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Use Limitation, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

A summary working description on each of the ten Fair Information Principles can be found below.

2.3.1 Accountability

Your company is responsible for the Personal Information it controls. Part of meeting this responsibility means that you must appoint someone to be accountable for compliance with PIPEDA.

To meet the accountability principle, if you haven't already, your company would do well to develop a privacy management program and relevant privacy policies. These should be reviewed at regular intervals to ensure ongoing compliance and staff should be trained to understand how their role intersects with your company's privacy requirements.

---

[3] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

2.3.2 Identifying Purposes

Your company's purposes for collecting users' Personal Information must be identified and documented before or at the time of collection. At the time of collection, individuals must be informed of the identified purpose, and if the purpose for processing that Personal Information changes, new consent must be obtained.

2.3.3 Consent

Before your company begins to collect, use, or disclose an individual's Personal Information, you must first collect and document each user's "meaningful consent." This means individuals must be informed of what they are consenting to, who the Personal Information is being shared with, and any potential risks.

The OPC highlights several conditions for collecting valid consent, including informing individuals in accessible ways, offering individuals the ability to withdraw consent, and ensuring the purposes for collection are considered appropriate.

2.3.4 Limiting Collection

Personal Information must be collected only for legitimate purposes and in a fair and lawful manner. Refer to the OPC's guidance on the 'Identifying Purposes' principle (s2.3.2) to make sure you're limiting the collection of Personal Information to what is necessary for the identified purpose.

2.3.5 Limiting Use, Disclosure, and Retention

Personal Information must only be used or disclosed for the purposes for which it was originally collected and kept only as long as required to fulfil those purposes.

To comply with this principle, it's important to understand what information your company has, where it is stored, and the purposes for its use or disclosure. Purposes for use and disclosure must be documented. For Personal Information that no longer fulfils a specified purpose, minimum and maximum retention periods should be applied

2.3.6 Accuracy

Your company is responsible for keeping Personal Information accurate, complete, and up-to-date. This can be fulfiled through the development of appropriate policies to keep the information updated and will help minimize the risk of inaccurate Personal Information being processed.

2.3.7 Safeguards

Personal Information must be protected through the implementation of effective security safeguards. When developing appropriate safeguards, consider the sensitivity of Personal Information and ensure it is protected from loss, theft, and unauthorised access. This can be achieved through technical or physical measures but must be reviewed periodically to ensure the safeguards remain appropriate.

2.3.8 Openness

To the greatest extent reasonable, take the information concerning your company's data handling policies and practices and make that information available to your customers (typically through your website). Public-facing policies, including your Privacy Notice, should be easy to access and easy to understand.

Where its feasible for your team to do it, make those documents accessible in multiple formats (e.g., writing, video) and inform your customers about how their information is used or disclosed, detailing who is responsible for privacy, and how individuals can submit a privacy complaint.

2.3.9 Individual Access

Individuals have the right to request access to their Personal Information and to contest its accuracy and completeness.

Companies must provide access to Personal Information upon users' request, in addition to explanations relating to where the information was collected, its specified purpose, and any disclosures that have been made.

Access to an individual's Personal Information must be provided free of charge and should be presented in several formats.

2.3.10 Challenging Compliance

Individuals can challenge your company regarding compliance with PIPEDA's ten principles. Communications of this nature should be made directly to the person working on behalf of your company that is responsible for privacy; and every complaint must be investigated.

Following a complaint, companies need to ensure that all complaints are documented and subsequent improvements to Personal Information handling practices are made. Individuals must be made aware of the outcome of the complaint and the steps taken to rectify the issue.

2.4 Establish a breach response process

PIPEDA includes mandatory breach reporting requirements that companiess must meet in certain circumstances. According to the OPC, a *breach* occurs when "there is a loss, unauthorised access to, use or disclosure of Personal Information." [4]

When a company's Safeguards are breached, they must assess whether the breach has posed a "real risk of significant harm." If it has, that company is required to report the breach to the OPC and notify the affected individuals and relevant third parties.

Mandatory breach reports must be made to the OPC; the report has to contain certain information relating to the incident and the steps taken after becoming aware of it.

Strong reporting and notification processes will help your company with compliance and accountability. However, it won't reduce the risk of reputational damage as a result of a breach.

---

[4] https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

As such, your company should develop an Incident Response Plan (IRP) to help soften that blow as much as possible.

3.0 Users' Privacy Rights

Individuals' privacy rights are a key part of most modern data protection and privacy laws. PIPEDA is no different and bears similarities to common privacy rights.

- **The Right to Access:** Individuals have the right to request access to information relating to the existence, use, and disclosure of their Personal Information. Companies must respond to an access request within a reasonable time frame and no later than 30 days from receipt. A response should be provided at minimal or no cost.

- **The Right to Correction:** Individuals have the right to request that the target company correct any inaccurate records of Personal Information they might have concerning that individual. Corrections must also be passed downstream to any third parties.

- **The Right to Withdraw Consent:** Individuals have the right to withdraw consent at any time. However, companies may retain Personal Information for the period necessary to fulfil the purpose for which it was collected.

- **The Right to Erasure:** The OPC has taken the position that individuals should have the ability to remove information that they have posted online; associated guidance from the OPC suggests that companies should include this right in relation to the right to withdraw consent.[5]

- **The Right to Lodge a Complaint:** Individuals have the right to file a complaint with the OPC if they believe a company's actions have violated PIPEDA.

- Finally, while the **"Right to be Informed"** is not explicitly discussed in PIPEDA, companies must nevertheless inform individuals of identified purposes for processing, either orally or in writing.

Companies covered (subject to) PIPEDA are required to include details of these privacy rights in their privacy notices, including how these rights can be exercised, and how individuals can verify their identity when making requests.

To ensure your business meets the 'Safeguards' principle (above), communication and fulfilment of privacy rights requests should be made through secure and encrypted channels (e.g., a web portal) and all requests should be documented to further demonstrate compliance.

---

[5] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos_or_201801/

Summary guidance about how to establish your company's workflows to properly process your users' privacy rights requests - also called 'data subject access requests' or 'DSARs' - is included in section 4.3 below.

4.0 Operationalise Your PIPEDA Compliance Program

4.1 Keep your Data maps current.

- Establish a data discovery process – This can be done manually, but an automated solution can yield faster and more accurate results
- Add classification and regulatory context – Ensure each type of data is classified correctly and the correct laws are being applied
- Review regularly – Schedule routine data map reviews and audits to ensure it is accurate and up to date with the latest regulations

4.2 Align your processing activities with the 10 FIPs.

- Understand your requirements – Ensure your company and its leadership team understands the principles they must apply to collect, use, and disclose Personal Information
- Align principles to processing activities – Assess whether each principle can be applied to existing or planned processing activities
- Inform – Ensure privacy notices are up to date and inform individuals about the purposes of the processing activities, how your company uses their Personal Information, and that they fully understand their data privacy rights.

4.3 Standardise and audit your DSAR processes.

- Intake – Provide an accessible privacy rights requests intake method
- Verification – Build an identity verification process or use a third-party service integration for your website (or app) to provide it.
- Discovery – Scan data maps for personal data related to the requestor
- Redaction – Remove any instances of personal data related to other individuals or proprietary information
- Respond – Deliver the request to the requestor via a secure portal in an accessible format

4.4 Establish & implement an incident response (IR) process.

- Intake – Provide an easily accessible intake method for incident reports
- Investigate – Investigate the incident. What has happened? What is the potential risk?
- Assess – Determine if the incident should be considered a breach

- Report – In the appropriate circumstances, make a report to the OPC, affected individuals, and third parties
- Remediate – Take the necessary steps to minimize the potential risk to affected individuals
- Document – Make a record of each incident report regardless of the severity

4.5 Get all your ducks in a row.

- Stay current – Keep on top of regulatory change to ensure your privacy program remains compliant
- Automate – Ditch manual processes for more streamlined automated solutions
- Everything all in one place – Use a centralised platform to embed PIPEDA compliance into your broader global privacy program and integrate with security, governance, and other teams
- Build trust – Go beyond compliance and what you have to do and start doing what you should do in order to build consumer trust

5.0 What Do I Do Next?

As you've navigated through this guide, we hope you've gained a deeper understanding of the PIPEDA compliance journey. While legally necessary, embracing PIPEDA should not merely be a ‘check the box’ activity. Rather, you and your company would stand to gain far more if you approach it with the mindset of bolstering customers’ trust in your services and protecting your customers' personal or otherwise confidential information — a fundamental aspect of data-driven business.

At True North PSR, we recognize that the path to PIPEDA compliance can seem daunting. If you determine you don’t have sufficient in-house resources to properly execute this project, this is where our expertise can make a crucial difference. Our team is ready to assist you at every step, ensuring that your compliance efforts are as seamless and efficient as possible. By partnering with us, you gain access to a wealth of knowledge and a partner who is as committed to securing your systems as you are.

Consider visiting our website at <www.TrueNorthPSR.com> to learn more about how we can help streamline your compliance program, ease the burden on your internal teams, and enhance your data privacy and security posture. We would be happy to help you turn the nuts and bolts of PIPEDA compliance into a strategic advantage for your business.