TRUELINE.IT

2026 PIPEDA Compliance Guide

Is Your Ontario Business Actually PIPEDA Compliant?

Trueline IT | Burlington, ON

Executive Summary

78% of Southern Ontario businesses we assessed lack a documented privacy policy that meets PIPEDA standards. If your business collects customer data — names, emails, phone numbers, IP addresses, employee records, purchase history, or financial data — you are legally required to comply with the Personal Information Protection and Electronic Documents Act (PIPEDA).

This guide explains what PIPEDA requires, walks through the 10 core principles, identifies the most common compliance gaps we see in Ontario businesses, and lays out a practical, ten-step path to compliance.

What PIPEDA Is — And Who It Applies To

PIPEDA is Canada's federal privacy law governing how for-profit organizations collect, use, and disclose personal information. Personal information includes any data that identifies an individual or could reasonably identify them. It does not apply to information held purely for personal, family, or household purposes — but any business data is squarely covered.

The 10 Core PIPEDA Principles

1. **Accountability.** Designate a privacy officer and document your privacy practices. You must be able to demonstrate compliance.
2. **Identifying Purposes.** Be clear about why you collect data before you collect it. Vague or undisclosed purposes violate PIPEDA.
3. **Consent.** Obtain explicit, informed consent from individuals before collecting or using their data. Pre-ticked boxes don't count.
4. **Limiting Collection.** Collect only the personal information you actually need for the stated purpose. Don't collect "just in case."
5. **Limiting Use.** Use data only for the purposes disclosed at collection. Any new use requires fresh consent.

6. Accuracy. Keep personal information accurate, complete, and up-to-date. Stale data is a compliance violation.

7. Safeguarding. Apply technical, physical, and organizational measures to protect data — encryption, access controls, and breach protocols.

8. Openness. Make privacy practices transparent and accessible. Your policy must be easy to find and understand.

9. Individual Access. Allow individuals to access their personal information and request corrections where inaccurate.

10. Challenging Compliance. Provide a process to file privacy complaints and challenge your compliance — you need a mechanism to handle disputes.

Where Ontario Businesses Fall Short

In our 2026 assessment of 20 Southern Ontario businesses across legal, accounting, financial, and healthcare sectors, we found the same gaps recurring everywhere:

- **No documented privacy policy — 78%.** Most businesses can't produce a policy that holds up to scrutiny.
- **Inadequate consent.** Data is collected without clear, documented consent mechanisms.
- **Unencrypted data.** Customer databases, shared passwords, and missing role-based access controls leave data exposed.
- **Indefinite retention.** Data is held forever without a documented justification or deletion schedule.
- **No breach protocol.** Most firms lack procedures for detecting, investigating, and reporting breaches — which is itself a legal requirement.
- **No staff training.** Employees aren't trained on privacy obligations or how to handle sensitive data securely.

10 Steps to Achieve PIPEDA Compliance

1. Conduct a privacy audit — map every type of personal data you collect, where it lives, who accesses it, and how long you keep it.

2. Document your privacy practices — publish a clear, plain-language privacy policy, easy to find on your website.

3. Implement consent processes — obtain explicit, informed consent for all data collection and honor opt-outs immediately.

4. Encrypt sensitive data — in transit (HTTPS) and at rest, including customer databases and backups.

5. Limit access — role-based access controls and multi-factor authentication; log who touches what data.

6. Create a data retention schedule — define how long each data type is kept, then securely delete on expiry.

7. Establish a breach response plan — detection, investigation, documentation, and reporting.

8. Train your team — annual privacy training so staff can identify and handle sensitive data correctly.

9. Appoint a privacy officer — someone accountable for oversight, complaints, and audits.

10. Review annually — audit compliance at least once a year and update as the business evolves.

What Happens If You Don't Comply

The Privacy Commissioner of Canada takes violations seriously. Non-compliance can lead to formal complaints, investigations, binding compliance orders, reputational damage, and liability for breaches.

The Commissioner holds the authority to issue findings of violation and enforcement orders — and enforcement is escalating. The Information and Privacy Commissioner of Ontario and the Canadian Centre for Cyber Security publish guidance that Ontario courts and insurers increasingly weigh.

How Trueline IT Helps

Compliance doesn't have to be overwhelming. We help Southern Ontario businesses assess current practices, build documented PIPEDA-aligned policies, implement encryption and access controls, define retention schedules, create breach-response procedures, and train staff — then keep it current with annual audits.

Trueline AI governance retainers start at **$1,500/month per business**, covering your AI Acceptable Use Policy, shadow AI audit, M365 configuration, and insurer-ready compliance documentation — no per-seat billing.

---

hello@truelineit.com | (647) 360-5774 | truelineit.com