PIPEDA Compliance Workbook

Companion to *PIPEDA Fundamentals* · Canuckt Privacy Academy Free course: canuckt.ai/learn/pipeda-fundamentals

This is the working half of the course. The course explains what the law requires; this workbook is where you write down what *your* organisation actually does, find the gaps, and decide who fixes them.

Work through it in order. Each section maps to one module of the course. Where a question asks for a name or a date, write one — "TBD" is the answer that ends up in a Commissioner's findings letter.

Print this, or fill it in on screen. There is nothing to submit and nobody collects it.

How to use it

Time	About 90 minutes if you know your systems. Longer the first time — that is the point.
Who should fill it in	Whoever can answer "where does personal information live". Usually not one person.
What you end up with	A gap list with owners and dates, which is the raw material of a privacy programme.
What it is not	Legal advice, or a filing. It is a self-assessment.

> **A note on honesty.** This workbook is only worth the time if you answer it as things are, not as you intend them to be. A gap you have written down is a gap you can close.

Section 1 — Does PIPEDA apply to you?

Module: What is PIPEDA?

1.1 Does your organisation collect, use or disclose personal information in the course of commercial activity? ☐ Yes ☐ No

1.2 Are you in Quebec, Alberta or British Columbia? ☐ Yes ☐ No If yes, substantially similar provincial legislation may apply to your intra-provincial activity instead. Name the law you believe applies: _____

1.3 Are you a federally regulated business — bank, airline, telecom, railway, inter-provincial transport? ☐ Yes ☐ No If yes, PIPEDA applies to you **regardless of province**.

1.4 Do you handle personal information of people outside Canada, or send it outside Canada? ☐ Yes ☐ No

1.5 — In one sentence, why does PIPEDA apply to you?

Section 2 — The 10 principles, scored honestly

Module: The 10 Fair Information Principles

Score each 0–3. **0** = we do not do this. **1** = ad hoc, undocumented. **2** = documented but not consistently followed. **3** = documented, followed, and evidenced.

#	PRINCIPLE	THE QUESTION TO ASK YOURSELF	SCORE
1	Accountability	Is there a *named* person responsible for privacy?	☐
2	Identifying Purposes	Can you state, per system, why you hold the data?	☐
3	Consent	Would the individual be surprised by what you do with it?	☐
4	Limiting Collection	Do you collect fields you never actually use?	☐
5	Limiting Use, Disclosure, Retention	Is there a retention period anyone enforces?	☐
6	Accuracy	Can an individual get an error corrected, and how fast?	☐
7	Safeguards	Encryption, access control, logging — for *this* data?	☐
8	Openness	Is your privacy policy findable and current?	☐
9	Individual Access	Could you answer an access request in 30 days today?	☐
10	Challenging Compliance	Does a complaint reach a human with authority?	☐

Total: _____ / 30

Your two lowest scores are your privacy programme for the next quarter. Write them here:

1. _____ Owner: __ **By:** ____
2. _____ Owner: __ **By:** ____

Section 3 — Consent

Module: Consent — Rules and Exceptions

3.1 For each way you collect personal information, record the consent you rely on.

WHERE YOU COLLECT IT	WHAT YOU COLLECT	EXPRESS OR IMPLIED?	IS THE PURPOSE STATED AT THE POINT OF COLLECTION?
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No

3.2 Sensitive information — health, financial, biometric — requires **express** consent. Do you collect any? ☐ Yes ☐ No If yes, list it and confirm the consent is express: _____

3.3 Can an individual withdraw consent? ☐ Yes ☐ No How, exactly — what do they click or who do they email? ____ What happens in your systems when they do? _____

3.4 — AI tools. Does personal information reach any AI tool — a chatbot, a summariser, a coding assistant, a meeting recorder? ☐ Yes ☐ No ☐ We do not know

> **"We do not know" is the most common honest answer, and it is a finding.** Shadow AI is where most Canadian organisations are currently out of compliance without knowing it. If you ticked it, that is gap number one.

Section 4 — Breach readiness

Module: Breach Notification Requirements

A breach is not the day you discover you were unprepared. Fill this in **before** you need it.

4.1 Who decides whether a breach creates a Real Risk of Significant Harm (RROSH)?

Name: ___ *Backup:* ___

4.2 Who reports to the Office of the Privacy Commissioner?

Name: ___ *Reached how, out of hours:* ___

4.3 The RROSH factors — the two PIPEDA names explicitly:

- Sensitivity of the information involved
- Probability the information has been, is being, or will be misused

Write your own worked example — a plausible breach for your organisation, and your RROSH call:

4.4 Record keeping. PIPEDA requires you to keep a record of **every** breach for **24 months** — including the ones that do not meet RROSH and are never reported.

Where does that record live? _____

Who writes it? ____ ☐ We do not currently keep one

4.5 Dry run. Date of your last breach walkthrough: __ **If that line is blank, book one:** ____

Section 5 — Access requests

Module: Individual Rights

5.1 An access request arrives by email today, addressed to nobody in particular.

- Who notices it? ____
- Who owns the response? ____
- **30 days** is the deadline. What day is your internal target? _____

5.2 Could you actually produce everything you hold on one named person?

☐ Yes, from a documented list of systems ☐ Probably, by asking around ☐ No

5.3 List every system that holds personal information. Keep going until it is boring.

SYSTEM	WHAT IT HOLDS	WHO CAN EXPORT FROM IT	RETENTION

> This table is a Record of Processing Activities in everything but name. If you fill in nothing else in this workbook, fill in this.

Section 6 — Cross-border transfers

Module: Cross-Border Data Transfers

6.1 Does personal information leave Canada? ☐ Yes ☐ No ☐ We do not know

6.2 For each provider outside Canada:

PROVIDER	WHAT IT PROCESSES	COUNTRY	CONTRACTUAL PROTECTION IN PLACE?
			☐ Yes ☐ No
			☐ Yes ☐ No
			☐ Yes ☐ No

6.3 PIPEDA does not prohibit transfers — it makes you **accountable** for them, and it requires **transparency**. Does your privacy policy tell people their data may be processed outside Canada? ☐ Yes ☐ No

6.4 The US CLOUD Act. Are any of the providers above US-controlled? ☐ Yes ☐ No If yes, note your assessment of that risk here — a reviewer will ask:

6.5 If you operate in Quebec, Law 25 requires a documented **privacy impact assessment before** a cross-border transfer. Have you done one? ☐ Yes ☐ No ☐ Not applicable

Section 7 — Your compliance checklist

Module: Enforcement and the Future

Tick only what is true today.

☐ A named individual is accountable for privacy, and they know it ☐ A current, findable privacy policy that matches what we actually do ☐ A list of every system holding personal information ☐ Documented retention periods that somebody enforces ☐ A written access-request procedure with a named owner ☐ A written breach-response procedure with an out-of-hours contact ☐ A breach log covering every incident, reportable or not, kept 24 months ☐ Consent language at each point of collection ☐ A record of which providers hold personal information, and where ☐ Staff have had privacy training in the last 12 months ☐ We know whether personal information reaches any AI tool ☐ Someone reviews all of the above on a schedule

Count of unticked boxes: _____

That number is your backlog. Take the top three into your next planning cycle.

Where to go next

- **Free course** — *PIPEDA Fundamentals*, 7 modules: canuckt.ai/learn/pipeda-fundamentals
- **Quebec** — Law 25 is stricter on consent, transfers and automated decisions: canuckt.ai/learn/law-25-guide
- **Email marketing** — CASL is a separate regime with separate penalties: canuckt.ai/learn/casl-guide
- **Doing this for a team** — Valdra tracks completion, keeps the evidence and produces the records above as living documents rather than a filled-in PDF: valdra.ai

---

This workbook is educational material, not legal advice. It reflects PIPEDA as at the date below. Where provincial legislation or PHIPA applies to you, additional obligations attach that this workbook does not cover.