

Privacy Program Readiness Checklist

A guide to preparing your organization for Bill C-36, and evolving Canadian privacy expectations*.

*Prepared with reference to Bill C-36 (first reading June 15, 2026). This checklist is for general readiness purposes and is not legal advice.

Introduction

Bill C-36, the proposed Protecting Privacy and Consumer Data Act (PPCDA), looks to modernize Canada's federal private-sector privacy framework and replace the Personal Information Protection and Electronic Documents Act (PIPEDA). This checklist allows you to assess your readiness for the requirements of the future PPCDA.

Accountability and Privacy Governance

- ☐ A named privacy lead is responsible for privacy compliance, questions and complaints.
- ☐ We maintain a practical privacy management program with policies, procedures, staff guidance and evidence that the program is operating.
- ☐ We know what personal information we hold and where that information resides.
- ☐ We treat information about children and youth as sensitive and apply safeguards and decision-making standards that reflect that sensitivity.
- ☐ We assess privacy implications before launching new systems, programs, digital tools or data-sharing initiatives.

Collection, Consent, and Transparency

- ☐ We collect only the personal information we need for clear, documented purposes.
- ☐ Privacy notices explain, in plain language, what information we collect, why we need it, how we use it, who we share it with and how long sensitive information is retained.
- ☐ Consent practices are meaningful and appropriate.
- ☐ We have a process to evaluate when an exception to consent may be relied upon and to document the rationale.
- ☐ We can respond to requests for access, correction and, where applicable, disposal or deletion of personal information within required timelines.
- ☐ We can explain to individuals whether information may be transferred outside Canada or across provincial borders.

Vendors, Tech and Cross-Border Data

- ☐ We know which vendors, cloud platforms and service providers process personal information on our behalf.
- ☐ Contracts require vendors to protect personal information to an appropriate standard and clearly address permitted uses (including, if applicable, AI uses), security, breach notification, retention and deletion.



- ☐ We understand where vendors store and process data, including the use of sub-processors and locations outside Canada.
- ☐ Before transferring personal information outside Canada, we assess the privacy risks and document appropriate mitigation measures.
- ☐ We review vendor privacy and security practices before procurement and periodically after implementation.
- ☐ We have a process to remove data from vendor systems when a contract ends or the information is no longer needed.

Retention, Security and incident Response

- ☐ Retention schedules define how long personal and other sensitive records are kept, based on purpose and legal requirements.
- ☐ Personal information is securely disposed of when it is no longer required.
- ☐ Physical, administrative and technical safeguards are proportionate to the sensitivity and volume of the information we hold.
- ☐ Access to sensitive information is role-based and reviewed periodically.
- ☐ We have a documented privacy breach and cybersecurity incident response process with clear escalation, notification and recordkeeping responsibilities.
- ☐ Employees know how to recognize and report a privacy incident, including accidental disclosure, phishing, lost devices and inappropriate AI use.

Training, Review and Continuous Improvement

- ☐ Privacy training is provided at onboarding and refreshed regularly for employees.
- ☐ Privacy policies, notices, vendor controls and operational procedures are reviewed at least annually and when material changes occur.
- ☐ We track privacy complaints, incidents, requests and recurring issues so that they lead to improvements in the program.
- ☐ Leadership receives enough information to understand material privacy risks and approve priorities for remediation.

