



PIPEDA Compliance Checklist

(Personal Information Protection and Electronic Documents Act)

For Canadian Small & Medium Enterprises (SMEs)

Prepared by IntelliSync Solutions

1. Accountability

- ■ Appoint a Privacy Officer responsible for compliance.
- ■ Document and maintain privacy policies and practices.
- ■ Train staff on privacy responsibilities.
- ■ Ensure third-party service providers follow PIPEDA.

2. Identifying Purposes

- ■ Clearly explain why personal information is collected.
- ■ Communicate purposes at or before time of collection.
- ■ Limit purposes to those that are necessary and lawful.

3. Consent

- ■ Obtain meaningful consent (clear, understandable).
- ■ Allow individuals to withdraw consent at any time.
- ■ Get explicit consent for sensitive information (e.g., health, finance).

4. Limiting Collection

- ■ Collect only information necessary for stated purposes.
- ■ Avoid gathering data 'just in case.'
- ■ Use fair and lawful means of collection.

5. Limiting Use, Disclosure & Retention

- ■ Use/disclose information only for identified purposes.
- ■ Get consent for new uses.
- ■ Have clear retention policies and securely dispose of data when no longer needed.

6. Accuracy

- ■ Keep personal information accurate and up-to-date.

- ■ Provide mechanisms for individuals to correct inaccuracies.

7. Safeguards

- ■ Apply safeguards based on sensitivity of information:
 - Physical (locked offices, restricted access)
 - Technological (encryption, firewalls, strong passwords)
 - Organizational (limited employee access, internal policies)
- ■ Regularly review and update security measures.

8. Openness

- ■ Make privacy policies publicly available (e.g., on your website).
- ■ Provide clear contact details for your Privacy Officer.

9. Individual Access

- ■ Respond to requests for personal information access within 30 days.
- ■ Provide access in understandable form.
- ■ Correct or amend personal data when requested.

10. Challenging Compliance

- ■ Establish a complaint-handling process.
- ■ Document and investigate privacy complaints promptly.
- ■ Inform individuals of their right to escalate complaints to the Office of the Privacy Commissioner of Canada (OPC).

Bonus: AI & Emerging Regulations (Bill C-27 – AIDA)

- ■ Assess whether AI systems using personal data are fair, transparent, and explainable.
- ■ Document risk assessments for bias, security, and misuse.
- ■ Implement data minimization and anonymization where possible.
- ■ Stay informed about the upcoming Artificial Intelligence and Data Act (AIDA).

■ **This checklist can be used as:**

- An internal compliance audit tool
- A policy development guide
- A training resource for employees