FREE RESOURCE — 2026 EDITION

PIPEDA Compliance Checklist for Ontario SMBs

50-Point Assessment Covering All 10 Fair Information Principles

DSIT Professional Services Inc. | dsitpro.com | Ontario, Canada

Purpose	Assess your organization's compliance with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
Applies To	All Canadian businesses that collect, use, or disclose personal information in the course of commercial activity
Last Updated	2026 — reflects current OPC guidance and Quebec Law 25 obligations
How to Use	Work through each section. Check items that are fully in place. Flag gaps for your remediation plan.

PRINCIPLE 1 — ACCOUNTABILITY

■ **Designated Privacy Officer named in writing**	Name and contact documented	■ **Privacy Officer responsibilities defined**	Written job description or policy
■ **Privacy policies reviewed annually**	Review date recorded	■ **Third-party data processors have written agreements**	Contracts include privacy clauses
■ **Staff aware of who the Privacy Officer is**	Communication on file		

PRINCIPLE 2 — IDENTIFYING PURPOSES

■ **Purpose for data collection documented before collection begins**	Written purpose statement	■ **Data collected is limited to what is necessary**	Minimization policy in place

■ **New data uses reviewed before implementation**	Change review process exists	■ **Purposes communicated to individuals at time of collection**	Consent form or notice used

PRINCIPLE 3 — CONSENT

■ **Consent obtained before or at time of collection**	Opt-in process in place	■ **Consent mechanism is clear and plain language**	Reviewed by non-legal staff
■ **Withdrawal of consent process documented**	Unsubscribe/opt-out functional	■ **Implied vs express consent distinction understood**	Policy addresses both
■ **Consent records retained**	Logs stored securely		

PRINCIPLE 4 — LIMITING COLLECTION

■ **Data inventory completed — all personal data mapped**	Inventory document exists	■ **Collection limited to what is necessary for stated purpose**	Minimization reviewed
■ **No collection of sensitive data without explicit justification**	Sensitive data defined		

PRINCIPLE 5 — LIMITING USE, DISCLOSURE, RETENTION

■ **Data not used for purposes beyond original consent**	Use audit completed	■ **Retention schedule documented for all data types**	Schedule reviewed annually
■ **Data destruction process defined and followed**	Destruction log maintained	■ **Third-party disclosures tracked and documented**	Disclosure log in place

PRINCIPLE 6 — ACCURACY

■ **Process for individuals to update their information exists**	Update request process documented	■ **Data accuracy reviewed periodically**	Review schedule set
■ **Inaccurate data corrected or flagged promptly**	Correction process documented		

PRINCIPLE 7 — SAFEGUARDS

■ **Encryption at rest implemented for personal data**	Encryption tool confirmed	■ **Encryption in transit implemented (TLS/HTTPS)**	SSL certificate valid
■ **Access controls limit data to need-to-know staff**	Role-based access reviewed	■ **MFA enabled on all systems containing personal data**	MFA audit completed
■ **Annual security assessment conducted**	Last assessment dated	■ **Physical access to data systems controlled**	Office/server room secured
■ **Portable device encryption enforced**	MDM policy in place		

PRINCIPLE 8 — OPENNESS

■ **Privacy policy publicly available on website**	URL documented	■ **Privacy policy written in plain language**	Readability reviewed
■ **Contact information for Privacy Officer published**	Available on website		

PRINCIPLE 9 — INDIVIDUAL ACCESS

■ **Process for handling access requests documented**	Response within 30 days	■ **Process for handling correction requests documented**	Correction process defined
■ **Staff trained on how to respond to access requests**	Training completed		

PRINCIPLE 10 — CHALLENGING COMPLIANCE

■ **Complaint process documented and communicated**	Process published	■ **Complaints logged and tracked**	Log maintained
■ **OPC contact information known to Privacy Officer**	opc.gc.ca bookmarked		

BREACH NOTIFICATION REQUIREMENTS

■ **Breach response plan documented**	Plan reviewed annually	■ **72-hour OPC notification requirement understood**	Threshold criteria defined
■ **Individual notification process defined**	Template letter drafted	■ **Breach log maintained**	Log includes date, scope, response
■ **Breach simulation / tabletop exercise completed**	Exercise date recorded		

QUEBEC LAW 25 ADDITIONAL OBLIGATIONS

■ **Privacy Impact Assessment (PIA) process in place**	Applies to new projects	■ **Data portability rights process documented**	Applies if Quebec customers served
■ **AI/automated decision-making disclosed to individuals**	If applicable	■ **Privacy Officer registration with Commission d'acces**	If Quebec residents' data held
■ **Cross-border data transfer agreements documented**	Applies to cloud services		

NEXT STEPS

Count your unchecked items. If you have 5 or more gaps, your organization has meaningful PIPEDA compliance exposure. DSIT Professional Services Inc. offers a free 30-minute compliance consultation to walk through your specific gaps and provide a prioritized remediation roadmap.

- Book your free compliance consultation: dsitpro.com/contact
- Download additional compliance resources: dsitpro.com/resources
- Learn more about DSIT's compliance services: dsitpro.com/compliance