GoCyberCheck

PIPEDA Quick-Check (SMB Privacy Readiness) — v1.1

Author: Seunguk (David) Ok · 2025-08-18 · Non-legal guidance; validate with counsel.

How to use this checklist

- Run quarterly and before major changes (new system/vendor/feature).
- Store artifacts under a shared path, e.g., /Privacy/PIPEDA/2025-Q3/.
- If an item is “No/Partial,” assign an owner/date and track in a gap log.
- Keep this checklist and artifacts for audit readiness.

1) Consent & Purpose Limitation

- Business purposes are identified for each data element.
- Privacy notice explains what/why and who to contact.
- Valid consent obtained (express or implied) appropriate to context.
- New purposes trigger re-assessment and notice/consent updates.

2) Collection & Minimization

- Only necessary data collected (minimization).
- Forms/fields reviewed annually to remove non-essential items.
- Sensitive data collection justified and documented.

3) Safeguards (Administrative, Physical, Technical)

- Least privilege with role-based access; access reviews at least quarterly.
- Strong authentication (e.g., MFA) on systems with personal information.
- Encryption in transit/at rest (where feasible); secure key management.
- Patch/vulnerability mgmt with SLAs; logged change control.
- Employee privacy/security training at least annually.

4) Access, Accuracy & Correction

- Process for access requests documented and published.
- Correction/updating process exists; downstream updates propagated.
- Response timelines and ID verification steps defined and followed.

5) Retention & Secure Disposal

- Retention schedules by data category are defined and applied.
- Secure deletion/shredding, including feasible backup handling.
- Disposal is logged (who/when/what) for auditability.

6) Breach Response & Notification

- IR plan includes privacy tasks (containment, assessment, evidence).
- Thresholds/workflows for notifying individuals, OPC, partners.
- Post-incident reviews feed lessons into playbooks.

7) Third Parties & Cross-Border Transfers

- Vendor list maintained with data categories, processing locations, DPAs.
- Due diligence + privacy/security clauses in contracts; reassessed annually.
- Cross-border transfers identified and addressed in notices/controls.

Evidence Examples (attach to your privacy folder)

- Privacy Notice — PDF or URL capture
- Consent Records — screenshots/logs with timestamps
- Access Reviews — quarterly attestations and remediation tickets
- Training Records — completion list and curriculum outline
- Retention Schedule — table per data category with disposal method
- Incident Playbooks — IR flow with privacy steps; last post-incident review
- Vendor Due Diligence — clauses, SOC 2/ISO certs, risk questionnaire
- Change Logs — patches, approvals, rollback plans (sample tickets)

Quick Tips for Small Teams

- Make a one-page RACI (owners for notice, consent, access reviews, vendors).
- Use consistent names (e.g., PRIV-CONSENT-2025-Q3.pdf).
- Shared drive: most staff read-only; editors limited by role.
- Track gaps in a simple sheet with owner/due date; review monthly.