Consulting

SMB Privacy Compliance Checklist

A plain-language guide for small and medium-sized businesses

This checklist helps SMBs identify where they stand on privacy compliance under Canadian federal and provincial legislation (PIPEDA, PIPA, PHIPA, LAW 25) and highlights areas of risk that may need professional attention. It is not legal advice.

🔴 **High Risk — Act immediately**	🟡 **Medium Risk — Plan a fix**	🟢 **Lower Risk — Monitor**	Use the Notes column to flag gaps or assign follow-up owners.

✓	Checklist Item	Risk	Notes / Action Owner
1. PRIVACY POLICY & NOTICES			
☐	**Privacy policy posted on your website** Must be accessible, clearly written, and reflect your actual data practices	High	*Notes:*
☐	**Privacy policy reviewed in the past 12 months** Policies must stay current with business changes and legislative updates	High	*Notes:*
☐	**Staff privacy notice or employee privacy policy in place** Employees have distinct privacy rights — separate policy required	High	*Notes:*
☐	**Collection notice at point of data collection** Users must know what is being collected and why before they provide it	Medium	*Notes:*
2. CONSENT & DATA COLLECTION			
☐	**Meaningful consent obtained before collecting personal information** Implied consent is increasingly insufficient — assess whether express consent is needed	High	*Notes:*
☐	**Website uses a compliant cookie consent banner**	Medium	*Notes:*

✓	Checklist Item	Risk	Notes / Action Owner
	Required for analytics, advertising, and tracking tools (especially if serving EU users)		
☐	**Email marketing list is CASL-compliant** Express or implied consent required; unsubscribe mechanism must function within 10 days	High	*Notes:*
☐	**Forms capture only information that is necessary for the stated purpose** Data minimization principle — do not collect more than you need	Medium	*Notes:*
☐	**Consent records are documented and stored** Be prepared to demonstrate consent was obtained if challenged	Medium	*Notes:*
3. DATA STORAGE, SECURITY & ACCESS			
☐	**Personal data is stored securely (encrypted, access-controlled)** Includes both digital files and physical records (paper files, printed reports)	High	*Notes:*
☐	**Access to personal data is limited to those who need it** Role-based access controls in place for CRM, HR systems, and shared drives	High	*Notes:*
☐	**Personal data is not stored on personal devices or unsecured cloud accounts** Includes employee phones, personal Gmail/Dropbox accounts, etc.	High	*Notes:*
☐	**Data retention schedule is defined and followed** Personal data must not be kept longer than necessary — includes deletion protocols	Medium	*Notes:*
☐	**Physical records (paper files) are secured and disposed of properly** Locked filing cabinets; shredding policy in place for disposal	Medium	*Notes:*

✓	Checklist Item	Risk	Notes / Action Owner
4. THIRD PARTIES & VENDORS			
☐	**All vendors that handle personal data on your behalf are identified** Includes payroll processors, CRM providers, cloud storage, marketing platforms	High	*Notes:*
☐	**Privacy or data processing agreements in place with key vendors** Contractual obligation to ensure vendors protect data appropriately	High	*Notes:*
☐	**Vendor data practices reviewed before onboarding** Know where data is stored (country matters for cross-border transfer rules)	Medium	*Notes:*
☐	**Data sharing with third parties is limited and purposeful** Do not share data with partners unless there is a lawful basis to do so	Medium	*Notes:*
5. INDIVIDUAL RIGHTS & REQUESTS			
☐	**Process in place to respond to access requests within 30 days** Individuals have the right to request access to their personal information	High	*Notes:*
☐	**Process to handle correction requests** Individuals can request their information be corrected if inaccurate	Medium	*Notes:*
☐	**Process to handle requests for deletion or withdrawal of consent** Especially important for marketing and customer databases	Medium	*Notes:*
☐	**Staff know how to recognize and escalate a privacy request** Requests may come by email, phone, or in person — all staff must know the process	Medium	*Notes:*

✓	Checklist Item	Risk	Notes / Action Owner
6. BREACH RESPONSE & INCIDENT MANAGEMENT			
☐	**Written data breach response plan exists** Defines roles, escalation steps, notification obligations, and documentation process	High	*Notes:*
☐	**Staff trained to recognize and report a suspected breach** Most breaches start with a phishing email, lost device, or accidental disclosure	High	*Notes:*
☐	**Breach notification obligations understood (PIPEDA, provincial)** Mandatory breach reporting thresholds differ by jurisdiction — know yours	High	*Notes:*
☐	**Breach log maintained even for incidents that do not require notification** PIPEDA requires a breach log regardless of notification outcome	Medium	*Notes:*
7. TRAINING & ACCOUNTABILITY			
☐	**A privacy officer (or accountable person) has been designated** Not required to be a lawyer or specialist, but must be assigned and known to staff	High	*Notes:*
☐	**Staff have received privacy awareness training in the past 12 months** Document training dates and participants for accountability purposes	Medium	*Notes:*
☐	**New staff receive privacy orientation as part of onboarding** Especially important for roles that handle customer or employee personal data	Medium	*Notes:*
☐	**Privacy is considered in new projects, tools, or service changes** Privacy by design: ask 'what data will this touch?' before launching anything new. Privacy Impact Assessment (PIA) required for Law 25.	Lower High	*Notes:*

What Your Results Mean

3+ High Risk items unchecked	Significant exposure. A privacy gap assessment and priority remediation plan is strongly recommended before you face a complaint, audit, or breach.
1–2 High Risk + multiple Medium items	Moderate risk. Prioritize the High Risk items and build a 90-day remediation roadmap for Medium items.
No High Risk checked, some Medium gaps	Good foundation. Schedule an annual review and consider a deeper privacy audit to validate your program.

Get a Free Privacy Risk Snapshot

If you identified gaps in this checklist, we can help. Contact us for a complimentary 30-minute Privacy Risk Snapshot — a structured conversation to identify your top three risks and a practical action plan.

Schedule your consultation with us today!

https://calendly.com/msing-ippconsulting/30min

This checklist is for general awareness purposes only and does not constitute legal advice. Privacy obligations vary by province, industry, and organization size. Consult a certified information privacy professional for guidance specific to your situation.