Canadian AI Compliance Quick-Reference Guide

For Private AI Infrastructure Decision-Makers

How to Use This Guide

This quick-reference guide helps Canadian IT leaders understand key compliance requirements when deploying AI infrastructure. Use it to:

- ☑ Identify which regulations apply to your organization
- ☑ Assess your current compliance posture
- ☑ Determine if private/on-premise AI infrastructure reduces regulatory risk
- ☑ Prepare for compliance audits and documentation requirements

This is not legal advice. Consult with legal counsel and compliance experts for specific guidance.

Part 1: Key Canadian AI & Data Regulations

CA Federal Level

Personal Information Protection and Electronic Documents Act (PIPEDA)

Applies to: Private sector organizations that collect, use, or disclose personal information in commercial activities

Key AI-Relevant Requirements:

- ☑ Consent for data collection and use
- ☑ Purpose limitation (use data only for stated purposes)
- ☑ Accuracy of personal information
- ☑ Security safeguards appropriate to sensitivity
- ☑ Openness about data management policies
- ☑ Individual access to their personal information
- ☑ Accountability (designate privacy officer)

AI Infrastructure Implications:

- Training AI models on customer data requires explicit consent
- Data used for AI must be accurate and up-to-date
- Cloud-based AI may involve cross-border data transfers (requires additional safeguards)
- On-premise AI infrastructure gives you full control over data location and security

---

Artificial Intelligence and Data Act (AIDA) - *Proposed*

Status: Part of Bill C-27 (pending as of 2025)

What It May Require:

- Risk assessments for high-impact AI systems
- Documentation of AI system design and development
- Human oversight mechanisms
- Transparency about AI decision-making
- Reporting of AI-related incidents

Preparedness Tip: Even before AIDA passes, documenting your AI governance framework positions you for compliance.

🏛 Provincial/Territorial Level

Quebec: Law 25 (An Act to Modernize Legislative Provisions Respecting Privacy Protection)

Enforcement Began: September 2023 **Penalties:** Up to $10M or 2% of global revenue (whichever is greater)

Key Requirements for AI:

- ☑ Privacy Impact Assessments (PIAs) for new technologies
- ☑ Data residency: Personal information of Quebec residents should remain in Quebec (or approved jurisdictions)
- ☑ Enhanced consent requirements
- ☑ Right to explanation for automated decisions
- ☑ Mandatory breach notification
- ☑ Privacy by design and by default

Why This Matters for AI:

- Cloud AI services (ChatGPT, Azure OpenAI, etc.) may store data outside Quebec
- Automated AI decisions require explanation mechanisms
- Private AI infrastructure in Quebec-based data centers simplifies compliance

---

British Columbia: Personal Information Protection Act (PIPA)

Applies to: Private sector organizations in BC

Key Points:

- Similar to PIPEDA but with BC-specific requirements
- Cross-border data transfers require consent or contracts
- AI systems processing BC resident data must meet PIPA standards

---

Alberta: Personal Information Protection Act (PIPA)

Applies to: Private sector organizations in Alberta

Key Points:

- Consent required for collection, use, and disclosure
- Security safeguards must be "reasonable"
- Cross-border transfers require notification or consent

Other Provinces/Territories

Most other provinces fall under federal PIPEDA for private sector organizations. However:

- Ontario is considering provincial privacy legislation
- Healthcare data may be subject to additional provincial health information acts (e.g., Ontario's PHIPA)

Part 2: Self-Assessment Checklist

☑ Compliance Readiness Scorecard

Rate your organization on each item (1 = Not Started, 5 = Fully Implemented):

Data Governance

☐ We have a documented data inventory (know what data we have, where it lives)
☐ We have a designated Privacy Officer or Data Protection Officer
☐ We have written policies for data collection, use, and retention
☐ We conduct Privacy Impact Assessments for new AI projects

Score: ___/20

Data Residency & Sovereignty

☐ We know where our data is physically stored (servers, cloud regions)
☐ We have documented which AI tools access our data and where they store it
☐ We have assessed cross-border data transfer risks
☐ We have contractual protections with cloud/AI vendors regarding data location

Score: ___/20

AI-Specific Controls

☐ We document the purpose and logic of AI systems that make automated decisions
☐ We can explain AI decisions to individuals when required
☐ We have human oversight mechanisms for high-impact AI decisions
☐ We have tested AI systems for bias, accuracy, and fairness

Score: ___/20

Security & Access Controls

- ☐ We have role-based access controls for sensitive data
- ☐ We encrypt data at rest and in transit
- ☐ We have incident response and breach notification procedures
- ☐ We regularly audit access logs and security configurations

Score: ___/20

Consent & Transparency

- ☐ We obtain explicit consent before collecting personal information for AI
- ☐ We inform individuals when AI is used to make decisions about them
- ☐ We have processes for individuals to access their data
- ☐ We have processes for individuals to request deletion or correction

Score: ___/20

📊 Your Total Score: ___/100

90-100: Strong compliance posture. Focus on continuous monitoring. **70-89:** Good foundation. Address gaps in weaker areas. **50-69:** Moderate risk. Prioritize documentation and governance. **Below 50:** High risk. Immediate action needed.

Part 3: Private AI Infrastructure & Compliance Benefits

How On-Premise AI Reduces Compliance Risk

Compliance Challenge	Cloud AI Risk	Private AI Advantage
Data Residency	Data may be processed in US or other jurisdictions	Full control—keep data in Canadian data centers
Cross-Border Transfers	Terms of Service may allow global processing	No transfers—data never leaves your infrastructure
Third-Party Access	Cloud vendors have technical access to your data	Zero third-party access—you control the keys
Breach Notification	Vendor breach may trigger your notification duty	You control security—fewer breach vectors
Audit Trail	Limited visibility into vendor's AI processing	Complete audit logs under your control
Right to Explanation	Vendor's model may be a "black box"	Deploy open-source models you can inspect
Data Deletion	Unclear if data is truly deleted from cloud	Physical deletion—verify data is gone

Part 4: Documentation Requirements

What to Prepare for Compliance Audits

☑ Privacy Impact Assessment (PIA) Template

- What data is collected and why
- How AI systems process that data
- Risks identified and mitigations implemented
- Data lifecycle (collection → storage → use → deletion)

☑ AI System Documentation

- Purpose and intended use of each AI system
- Data sources and training methodology
- Accuracy testing and bias mitigation steps
- Human oversight and review processes

☑ Data Processing Agreements

- Contracts with any vendors who access your data
- Terms covering data location, security, and deletion
- Subprocessor disclosure (who else touches your data)

☑ Consent Records

- How consent was obtained (forms, checkboxes, etc.)
- What consent covers (specific purposes)
- How individuals can withdraw consent

☑ Incident Response Plan

- Who to notify in case of a breach
- Timeline for notification (72 hours in some cases)
- Steps to contain and remediate

Part 5: Key Questions to Ask Vendors

Cloud AI Provider Evaluation

Before deploying cloud-based AI, ask your vendor:

❓ **Where is our data physically stored?** (Specific data centers, not just "North America")

❓ **Do you transfer data across borders for processing?** (Even temporarily?)

❓ **Who has access to our data?** (Vendor employees, subprocessors, support teams?)

❓ **Can you guarantee data deletion upon request?** (How do you verify?)

❓ **Do you use our data to train your models?** (Opt-out available?)

❓ **What certifications do you hold?** (SOC 2, ISO 27001, etc.)

❓ **Do you comply with Quebec Law 25 and PIPEDA?** (Get it in writing)

❓ **What is your breach notification policy?** (How quickly will you tell us?)

Part 6: Action Plan for Compliance

30-Day Quick Wins

☑ Week 1: Assess

- Complete the Compliance Readiness Scorecard (Part 2)
- Identify your 3 biggest gaps
- Document which regulations apply to your organization

☑ Week 2: Inventory

- Create a data inventory (what data, where stored, who accesses)
- List all AI tools currently in use (including shadow AI)
- Map data flows (where data enters, how it's processed, where it exits)

☑ Week 3: Document

- Draft or update your Privacy Policy
- Create a simple AI Governance Framework document
- Document consent mechanisms

☑ Week 4: Plan

- Identify quick compliance improvements (e.g., encrypt data at rest)
- Evaluate whether private AI infrastructure reduces your risk
- Schedule a discovery call with Optrics to explore on-premise options

---

90-Day Strategic Actions

☑ Governance

- Designate a Privacy Officer or AI Ethics Lead
- Establish an AI Review Committee
- Create approval workflows for new AI projects

☑ Technical Controls

- Implement encryption and access controls
- Set up audit logging for AI system access
- Test AI systems for accuracy and bias

☑ Vendor Management

- Review contracts with cloud AI providers
- Require Data Processing Agreements with all vendors
- Audit third-party access to your data

☑ Training

- Train employees on privacy and AI ethics
- Document who has completed training
- Create an AI Acceptable Use Policy

Part 7: Resources & Next Steps

Where to Learn More

Regulatory Authorities:

- CA **Office of the Privacy Commissioner of Canada (OPC):** www.priv.gc.ca
- 🏛 **Commission d'accès à l'information (Quebec):** www.cai.gouv.qc.ca

Industry Guidance:

- **CIO Strategy Council:** AI governance frameworks
- **Standards Council of Canada:** AI standards development

Legal Resources:

- Consult with privacy lawyers specializing in Canadian AI compliance
- Consider joining industry associations (e.g., IAPP Canada)

🚀 Next Step: Book Your Discovery Call

If this checklist revealed compliance gaps, or if you're considering private AI infrastructure to reduce regulatory risk, **let's have a conversation.**

What you'll get in your 15-minute discovery call:

- Assessment of your compliance readiness
- Guidance on whether on-premise AI infrastructure makes sense
- Realistic timeline and budget expectations
- No pressure - just expert advice

Book your call:

Online form: https://Content.Optrics.com/Dell-AI-Factory

You can also call us at **1-877-430-6240** or email as at Info@Optrics.com.

About This Guide

Created by: Optrics Engineering **Purpose:** Educational resource for Canadian IT leaders exploring AI infrastructure options **Last Updated:** October 2025 **Disclaimer:** This guide provides general information only and does not constitute legal advice. Consult with qualified legal and compliance professionals for specific guidance.

Questions?

✉ Email: Info@Optrics.com
📞 Phone: 1-877-430-6240
🌐 Web: www.Optrics.com

Optrics Engineering | DELL Technologies AUTHORIZED PARTNER