

ATIA/POPA AI Compliance Checklist for Alberta Municipalities

Alberta's modernized Access to Information Act (ATIA) and Protection of Privacy Act (POPA) require every public body — including municipalities of any size — to implement a formal Privacy Management Program. The compliance deadline was June 11, 2026. Each item below is a required component. If any does not exist in your organization as a written, adopted document, you have a gap.



1. Designated Privacy Officer

Formally designate a Privacy Officer in writing — a council resolution or administrative order. This person receives access requests, manages breaches, and is accountable for the Privacy Management Program. The designation must be documented.



2. Personal Information Inventory

Map every location where your municipality collects, uses, or discloses personal information — paper records, software systems, cloud services, and the AI tools staff are using. Shadow AI tools belong in this inventory.



3. Plain-Language Privacy Policy

A written, public policy explaining what personal information you collect, why, how you protect it, and how individuals can access or correct their records. It must reference ATIA and POPA explicitly and be posted on your website at minimum.



4. AI Acceptable Use Policy

A formal policy governing staff use of AI tools: which tools are sanctioned, which are prohibited, what data may and may not be entered into AI systems, and the consequences of unauthorized use. This is the document that addresses shadow AI directly.



5. Breach Response Procedures

Written, step-by-step procedures: who is notified, in what timeframe, what records are kept. POPA requires notification to the Privacy Commissioner and affected individuals for breaches creating a real risk of significant harm.



6. Staff Training Records

Documented evidence that staff who handle personal information have received privacy and AI use training — who was trained, when, and on what content. Training records are a required component, not just a best practice.



7. Third-Party Vendor Agreements

Review every software contract, cloud service, and vendor relationship involving personal information. Flag any AI vendors — including Microsoft Copilot or Google Workspace AI — processing citizen data without an executed data processing agreement.



8. Documented, Council-Adopted Program

Compile the above into a single Privacy Management Program document, dated and adopted by council, with at minimum an annual review cycle. Update it whenever your technology stack changes — including every new AI tool.

Not sure where your municipality stands?

Spencer Morley Consulting runs AI readiness assessments and builds compliant Privacy Management Programs for Alberta municipalities. Book a call at calendly.com/jordan-spencermorleyconsulting or email jordan@spencermorleyconsulting.ca.