KIRKE CONSULTING

Empowering transformation through expertise

ALBERTA PRIVACY COMPLIANCE & MANAGEMENT CHECKLIST

This checklist supports Alberta public bodies in operationalizing their obligations under the Protection of Privacy Act ("POPA") and associated regulations. It translates legislative requirements into practical, actionable steps to help leadership, privacy officers, and operational teams establish, implement, and maintain a Privacy Management Program ("PMP") in accordance with Section 25 of POPA.

Establish Legislative and Compliance Context

- Confirm whether the organization is subject to Alberta privacy legislation (e.g., as a public body or a private organization).
- Identify applicable statutes, regulations, directives, and guidance from oversight bodies.
- Monitor for legislative or regulatory changes and update practices accordingly.
- Establish Roles and Responsibilities.
- Appoint a Privacy Officer or equivalent with clear authority and resources.
- Secure leadership support and executive or board-level oversight for privacy compliance.
- Define and document roles and responsibilities related to the collection, use, disclosure, retention, correction, and safeguarding of personal information ("PI").
- Establish escalation and decision-making processes for privacy risks and incidents.

PI Inventory & Records Management

- Identify and document all PI collected, including sensitive information.
- Maintain an inventory of systems, applications, vendors, and physical locations where PI is stored or processed (electronic and paper).
- Identify cross-border PI storage or access, if applicable.
- Maintain and publish (where required) a directory or description of Personal Information Banks (PIBs) or equivalent records.
- Establish and maintain a security classification scheme for PI

Verify Vendor Compliance

- Review agreements with vendors to ensure they include PI protection requirements.
- Confirm vendors have documented breach notification procedures.
- Add or update privacy and security schedules in agreements where gaps exist.
- Periodically reassess vendor compliance and risk.

KIRKE CONSULTING

Empowering transformation through expertise

ALBERTA PRIVACY COMPLIANCE & MANAGEMENT CHECKLIST

Privacy & Collection Notice Requirements

- Identify and document legal authority for collection of PI.
- Provide individuals with clear notice at or before the time of collection, including the purpose of collection, legal authority, contact information for inquiries, and disclosure of any automated processing.
- Publish an external privacy notice outlining:
    - Types of PI collected,
    - Why and how PI is used,
    - Any disclosures (e.g., to service providers),
    - Individual rights (access, correction),
    - Contact information for questions.
- Develop and communicate an internal or employee privacy notice.

Document PMP

- Create a written Internal Privacy Policy
- Develop Privacy Breach procedures for breach identification, containment, notification, and reporting.
- Create Records Retention Policy, schedules and PI classification schemes
- Document the Privacy Impact Assessment procedure, including when a PIA is required, how it is completed, and requirements for engaging the Privacy Commissioner.
- Establish process to make the PMP publicly accessible on request.

Privacy Impact Assessments

- Conduct PIAs in all prescribed circumstances (e.g., new technologies, significant changes) involving PI.
- Track completed PIAs and ensure mitigation measures are implemented and reviewed.

Implement Privacy Training and Awareness

- Deliver privacy training at least annually to employees, contractors, volunteers, and leadership.
- Tailor training based on roles and access to PI.
- Maintain records of training participation and updates.

KIRKE CONSULTING

Empowering transformation through expertise

ALBERTA PRIVACY COMPLIANCE & MANAGEMENT CHECKLIST

Manage Use of PI & PI Matching

- Prohibit all sales of PI.
- Establish controls and security safeguards for PI matching, analytics, or synthetic PI creation.
- Keep records for all PI anonymization efforts.
- Periodically review PI practices to ensure alignment with stated purposes and authority.

Artificial Intelligence & Automated Decision-Making (Where Applicable)

- Identify whether the organization uses automated systems or artificial intelligence involving PI, data derived from PI, or non-personal data.
- Establish policies governing the use of AI (where applicable).
- Disclose the use of automated decision-making in privacy notices, where required.