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, and maintain a Privacy Management Program ("PMP") in accordance with Section 25 of POPA.

Governance & Program Foundation

- ✓Confirm the Division is subject to POPA and ATIA as an Alberta public body; identify all applicable statutes, regulations, and OIPC guidance.
- ✓Appoint an Access and Privacy Officer with documented authority, resources, and executive oversight.
- ✓Define and document roles and responsibilities for collection, use, disclosure, retention, correction, and safeguarding of PI.
- ✓Establish escalation and decision-making processes for privacy risks, incidents, and complaints.
- ✓Implement a written PMP proportional to the volume and sensitivity of PI held; make it publicly available on request.

PI Inventory, Classification & Retention

- ✓Identify and document all PI collected, including sensitive categories (biometric, financial, minors).
- ✓Maintain an inventory of all systems, applications, vendors, and physical locations where PI is stored or processed, including any cross-border storage.
- ✓Assign a security classification level to all PI, derived data, and non-personal data based on sensitivity; apply proportionate controls.
- ✓Maintain a Personal Information Bank (PIB) directory for all PI collections; make it available on request.
- ✓Establish retention schedules and secure disposal procedures for PI and records.

Safeguards & Vendor Management

- ✓Implement documented administrative, technical, and physical safeguards appropriate to the sensitivity and volume of PI, including proactive monitoring of information systems.
- ✓Review vendor agreements to include PI protection requirements and breach notification procedures; add or update privacy schedules where gaps exist.
- ✓Establish controls for PI matching, analytics, and synthetic PI creation; keep records of all anonymization efforts and prevent re-identification.

Artificial Intelligence & Automated Decision-Making (Where Applicable)

- ✓Maintain an inventory of all AI systems and automated decision systems used by the Division involving PI or derived data.
- ✓Require a PIA before before deploying any new or materially changed AI system involving PI.
- ✓Document safeguards, human oversight, and bias controls in an AI Governance Policy.
- ✓Disclose the use of automated decision-making in privacy and collection notices.

© KIRKE MANAGEMENT CONSULTING. ALL RIGHTS RESERVED.

KIRKE CONSULTING

Empowering transformation through expertise

ALBERTA PRIVACY COMPLIANCE & MANAGEMENT CHECKLIST

Collection, Notice & Consent

- ✓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 Procedures PMP

- ✓Create a written Internal Privacy Policy.
- ✓Develop Privacy Breach procedures for breach identification, containment, notification, and reporting.
- ✓Establish retention schedules and disposal procedures for PI; document secure disposal methods for both electronic and paper records.
- ✓Create Records Retention Policy, schedules and PI classification schemes.
- ✓Develop a Privacy Rights Management Procedure covering access requests, correction requests, complaint handling, privacy rights fees, and OIPC referral.
- ✓Document the Privacy Impact Assessment procedure, including when a PIA is required.
- ✓Document the Division's approach to creating, using, and disclosing non-personal data and data derived from personal information.
- ✓Prohibition of all sales of PI.
- ✓Establish process to make the PMP publicly accessible on request.

Implement Privacy Training and Awareness

- ✓Deliver role-proportionate privacy training to all staff, contractors, volunteers, and leadership at least annually; tailor content based on access to PI.
- ✓Provide privacy orientation to new employees at onboarding covering key obligations, Division procedures, and staff responsibilities.
- ✓Document and track training completion, retraining deadlines, and role-based requirements.

Privacy Impact Assessments

- ✓Conduct PIAs in all prescribed circumstances.
- ✓Track completed PIAs; confirm mitigation measures are implemented and periodically reviewed.

© KIRKE MANAGEMENT CONSULTING. ALL RIGHTS RESERVED.