Arann Tech Bill C-27 Readiness Audit Checklist

https://aranntech.com/

Operational Assessment for CPPA Alignment (Pre-Enactment)

Purpose:
This checklist is designed to help organizations evaluate whether their current privacy, security, and data operations are capable of meeting the
It focuses on provable capability, not policy intent.

Section 1: Governance & Accountability

Privacy Ownership

- [ ] A designated privacy lead exists with decision authority (not advisory only)
- [ ] Privacy responsibilities are formally documented and approved by leadership
- [ ] Escalation paths are defined for privacy incidents and regulator inquiries

Privacy Management Program (PMP)

- [ ] A written Privacy Management Program exists (not just a privacy policy)
- [ ] The PMP includes staff training, complaint handling, breach response, and review cycles
- [ ] The PMP is reviewed at least annually or after major operational changes

Board and Executive Oversight

- [ ] Privacy risk is reported to executive leadership at least once per year
- [ ] Privacy is included in enterprise risk assessments
- [ ] Material privacy incidents trigger executive review

Section 2: Data Mapping & Visibility (Critical)

Personal Data Inventory

- [ ] A current inventory of personal data exists across systems, cloud services, and vendors
- [ ] Data flows are mapped from collection to deletion
- [ ] Shadow IT and local data stores are included in scope

Purpose Limitation

- [ ] Each dataset has a documented business purpose
- [ ] Data not tied to a valid purpose is flagged for deletion or anonymization

Third-Party Data Exposure

- [ ] All vendors processing personal data are documented
- [ ] Data shared with vendors is limited to minimum necessary
- [ ] Vendor data locations and retention practices are known

Section 3: Consent & Legitimate Interest Readiness

Consent Clarity

- [ ] Consent notices are written in plain language for the intended audience
- [ ] Consent mechanisms are auditable and time-stamped
- [ ] Withdrawal of consent is operationally possible

Legitimate Interest Assessments

- [ ] Legitimate interest use cases are explicitly identified
- [ ] Privacy Impact Assessments (PIAs) exist for each use case
- [ ] Balancing tests are documented and approved internally

Section 4: Individual Rights Fulfillment (High Risk Area)

Access and Correction

- [ ] Requests can be fulfilled within statutory timelines
- [ ] Identity verification is built into request workflows
- [ ] Responses are logged and auditable

Right to Disposal (Deletion)

- [ ] Deletion workflows exist across production systems
- [ ] Backup and archive implications are understood
- [ ] Exceptions to deletion are documented and defensible

Data Mobility

- [ ] Personal data can be exported in a structured, commonly used format
- [ ] Export does not expose third-party or internal metadata

Section 5: Security Safeguards & Breach Readiness

Technical Safeguards

- [ ] Access controls follow least-privilege principles
- [ ] Administrative access is logged and reviewed
- [ ] Backup systems are isolated from production access

Breach Detection

- [ ] Security events are monitored, not just logged
- [ ] Alerting exists for unauthorized access to personal data
- [ ] Incident response roles are clearly defined

Breach Response

- [ ] Breach response plans are documented and tested
- [ ] Risk of Significant Harm (RROSH) can be assessed quickly
- [ ] Breach notification workflows are rehearsed

Section 6: Vendor & Processor Controls

Contractual Safeguards

- [ ] Vendor contracts include privacy and security obligations
- [ ] Vendors are required to assist with deletion requests
- [ ] Breach notification timelines are contractually defined

Ongoing Vendor Risk

- [ ] Vendors are reviewed periodically, not only at onboarding
- [ ] High-risk vendors receive enhanced monitoring
- [ ] Termination procedures include data return or destruction

Section 7: Automated Decision Systems & AI (If Applicable)

System Identification

- [ ] Automated systems impacting individuals are documented
- [ ] Decision logic inputs and outputs are understood at a high level

Transparency Readiness

- [ ] Explanations can be provided in plain language upon request
- [ ] Vendor-supplied AI systems support transparency requirements

AIDA Awareness

- [ ] High-impact AI use cases are identified
- [ ] Governance ownership for AI risk is assigned

Section 8: Evidence & Audit Readiness

Documentation

- [ ] Policies match actual technical controls
- [ ] Logs demonstrate enforcement, not just intent
- [ ] Historical decisions are traceable

Operational Proof

- [ ] Deletion requests have been tested end-to-end
- [ ] Breach simulations have been conducted
- [ ] Staff know how to route privacy requests correctly

Final Readiness Assessment

- [ ] No critical gaps in deletion capability
- [ ] No unknown personal data stores
- [ ] No vendors processing data without contracts
- [ ] No reliance on policy without technical enforcement

Overall Readiness Status

- [ ] High: Capable of meeting CPPA enforcement expectations
- [ ] Moderate: Requires targeted remediation
- [ ] Low: Significant operational exposure

How to Use This Checklist

- Treat unchecked items as operational risk, not legal theory
- Prioritize visibility, deletion capability, and vendor control
- Document remediation actions and timelines

Important Note

This checklist supports operational readiness and risk assessment. It does not replace legal advice. Organizations should consult qualified legal counsel regarding statutory interpretation and obligations.