Privacy Assessment Checklist

Use this standardized checklist to create a privacy assessment process for regular reviews and analysis of impact of risk on personal information, in compliance with PIPEDA, PHIPA, GDPR, Law 25 & other data protection requirements.

Fair Information Principles In Canada

1. Accountability

- Assign Responsibility: Designate a privacy officer or team responsible for compliance with privacy principles and conducting PIAs.
- Develop Policies: Establish and implement privacy policies and procedures that comply with relevant legislation and standards.
- Training: Provide regular training to employees on privacy policies and the importance of PIAs.

2. Identifying Purposes

- Purpose Specification: Clearly define and document the purposes for which personal data is being collected, used, and disclosed.
- Review and Update: Regularly review and update the specified purposes to ensure they remain relevant and lawful.

3. Consent

- Informed Consent: Obtain explicit consent from individuals for the collection, use, and disclosure of their personal data.
- Withdrawal of Consent: Provide easy-to-understand methods for individuals to withdraw their consent at any time.
- Record Keeping: Maintain records of consent obtained from individuals.

4. Limiting Collection

- Data Minimization: Collect only the personal data necessary to fulfill the specified purposes.
- Collection Methods: Use lawful and fair means to collect personal data, ensuring transparency with individuals.

5. Limiting Use, Disclosure, & Retention

- Use Limitation: Use personal data only for the purposes for which it was collected, unless further consent is obtained.
- Retention Policy: Establish and adhere to data retention policies that specify how long personal data is kept and the secure disposal of data no longer needed.
- Third-Party Agreements: Ensure third-party service providers comply with privacy requirements through binding agreements.

6. Accuracy

- Data Quality: Ensure personal data is accurate, complete, and up-to-date.
- Regular Audits: Conduct regular audits and reviews to verify the accuracy and quality of personal data.

7. Safeguards

- Security Measures: Implement appropriate physical, technical, and administrative security measures to protect personal data against unauthorized access, disclosure, alteration, and destruction.
- Access Controls: Limit access to personal data to authorized personnel only.
- Incident Response: Establish an incident response plan to address data breaches and other security incidents promptly.

8. Openness

- Transparency: Make information about privacy policies, procedures, and practices readily available to individuals.
- Communication: Regularly communicate with individuals about how their personal data is being handled.

9. Individual Access

- Access Requests: Provide individuals with the right to access their personal data and obtain information about its processing.
- Correction Requests: Allow individuals to request corrections to their personal data if it is inaccurate or incomplete.

10.Challenging Compliance

- Complaint Handling: Establish procedures for individuals to challenge compliance with privacy principles and address their complaints.
- Review Mechanism: Implement a mechanism for reviewing and resolving privacy-related complaints and disputes.

Steps to Complete a Privacy Impact Assessment (PIA)

1. Prepare for the PIA

- ❑ Identify Need for PIA: Determine whether a PIA is necessary for the system, application, or process being developed or modified.
- ❑ Gather Team: Assemble a team of stakeholders, including privacy officers, legal experts, IT professionals, and business unit representatives.

2. Describe the Project

- ❑ Document Project Details: Provide a detailed description of the system, application, or process, including its purpose, scope, and functionalities.
- ❑ Identify Data Flows: Map out how personal data will be collected, used, stored, and shared within the project.

3. Identify and Analyze Privacy Risks

- ❑ Risk Identification: Identify potential privacy risks associated with the project, considering factors such as data sensitivity, volume, and processing activities.
- ❑ Risk Analysis: Assess the likelihood and impact of identified risks on individuals' privacy.

4. Evaluate Mitigation Measures

- ❑ Existing Controls: Review existing security and privacy controls to determine their effectiveness in mitigating identified risks.

- ❑ Additional Measures: Recommend additional measures to address any gaps and enhance privacy protection.

5. Document the PIA Findings

- ❑ PIA Report: Compile the findings of the PIA into a comprehensive report that includes an overview of the project, identified risks, and mitigation measures.
- ❑ Review and Approval: Submit the PIA report for review and approval by relevant stakeholders and decision-makers.

6. Implement and Monitor Mitigation Measures

- ❑ **Action Plan**: Develop an action plan to implement the recommended mitigation measures.
- ❑ **Ongoing Monitoring**: Continuously monitor the project to ensure that privacy risks are managed effectively and that mitigation measures remain effective.

Other Recommendations for Privacy Impact Assessments

- **Regular Updates**: Conduct regular PIAs and update them as needed to reflect changes in data processing activities and legal requirements.
- **Stakeholder Involvement**: Involve relevant stakeholders, including legal, IT, and business units, in the PIA process to ensure comprehensive assessments.
- **Documentation**: Maintain detailed documentation of the PIA process, findings, and actions taken to address privacy risks.

- **Continuous Improvement**: Regularly review and improve PIA practices to enhance privacy protection and compliance.

Let's discover how easy a managed PIA can be:
https://www.privacyassessment.ca