# POLICIES AND PRACTICES FRAMING THE GOVERNANCE OF PERSONAL INFORMATION BY CERBA RESEARCH CANADA

(Document to be published on Cerba Research's website)

| A. Building Blocks of the Governance Program | | |
|---|---|---|
| **Organizational Commitment** | **a) Senior Management Buy-In** | Senior management support the Personal Information Governance Program and promotes a privacy-friendly culture by:<br>• Appoint the Privacy Officer (PO);<br>• Approve program control measures;<br>• Monitor the program and report to the Board as appropriate;<br>• Provide the resources necessary to ensure the success of the program. |
| | **b) Privacy Officer** | Responsible for the development and implementation of program controls and their ongoing assessment and review. |
| | **c) Reporting** | The organization has established accountability mechanisms and reflect them in its program controls. |
| **Governance Program Controls** | **a) Personal Information Inventory** | The organization is able to identify:<br>• PI in its custody or control;<br>• Purposes for collecting, using and disclosing PI;<br>• The sensitivity of PI;<br>• Security measures in place. |
| | **b) Policies** | • PI protection policy which details the role and responsibilities of staff members throughout the lifecycle of this information;<br>• Directive on collection, use and disclosure of PI;<br>• Directive on retention, destruction and anonymization of PI;<br>• Directive on security measures for PI;<br>• Procedure for handling requests and complaints relating to PI; |

| | | |
|---|---|---|
| | | • Procedure for managing confidentiality incident involving PI;<br>• Privacy policy for PI collected through the website. |
| | **c) Risk Assessment Tools** | Privacy Impact Assessment (PIA) for:<br>• Any project to acquire, develop or overhaul an information or electronic service delivery system involving the collection, use, disclosure, retention, or destruction of PI;<br>• Disclosing Personal Information outside Quebec or entrusting a third party located outside Quebec with the task of collecting, using, disclosing or retaining Personal Information on its behalf;<br>• Disclosing Personal Information to a third party without the consent of the persons concerned for a study, research, or statistical production.<br>Risk of serious harm assessment grid for confidentiality incident. |
| | **d) Training and education** | A training program which targets all employees, including managers, and cover namely the following topics:<br>• Applicable laws and internal policies-directives-procedures regarding the protection of PI;<br>• Techniques to identify and recognize potential confidentiality incidents;<br>• Handling of privacy complaints and requests;<br>• The consequences of violating privacy laws and internal rules. |
| | **e) Confidentiality incident management protocol** | The organization has established a procedure and appointed a person responsible for the management of confidentiality incidents involving PI. Responsibilities for internal and external reporting of violations have been clearly defined.<br>The organization maintains a register of all confidentiality incidents, even those that do not involve a risk of serious harm. |
| | **f) Service Provider Management** | The organization includes privacy clauses or enter into a data processing agreement which includes:<br>• PI Protection measures; |

| | | |
|---|---|---|
| | | • The use of PI for the purpose of contract performance;<br>• Destruction of PI at the end of the contract;<br>• The obligation of the service provider to promptly notify the organization of any breach or attempted breach of confidentiality obligations;<br>• The ability of the organization to request any document and conduct any audit related to the confidentiality of PI. |
| | **g) External communication** | The organization informs individuals of their rights to privacy protection and the controls of its governance program. The privacy policy on the organization's website is written in plain and clear language and include the following:<br>• The purpose of the collection, use and disclosure of PI and its protection and retention period;<br>• Inform individuals if their PI is being disclosed outside of Quebec;<br>• PO's contact information for questions, requests or complaints. |
| **B. Ongoing Assessment and Revision** | | |
| **Oversight and Review Plan** | The organization has developed an oversight and review plan on an annual basis that sets out how it monitors and assesses the effectiveness of the organization's program controls. | |
| **Assess and Revise Program Controls as Necessary** | 1. Update the PI inventory;<br>2. Reviewing policies, directives, and procedures;<br>3. Treat risk assessment tools as living documents;<br>4. Modify training and educations courses;<br>5. Adapt confidentiality incident management protocol;<br>6. Refine the service provider management;<br>7. Improve external communications. | |