Privacy Management Program – *A Practical Checklist for Compliance*

The Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia jointly released a 26-page guidance document in April 2012 entitled, "Getting Accountability Right with a Privacy Management Program"

IAB Canada's partner in Policy and Regulatory Affairs, Osler developed the following checklist. It is derived from guidelines established by the Canadian Privacy Regulatory Authorities in "Getting Accountability Right with a Privacy Management Program"

The guidance document sets out these Canadian privacy regulatory authorities' joint expectations for organizational privacy management programs. Specifically, the guidance states that, during the course of an investigation or audit, the Canadian privacy regulatory authorities will "expect that organizations can demonstrate that they have an up-to-date, comprehensive privacy program in place."

IAB Canada is sharing this chart summarizing the requirements for privacy management programs as they are detailed in the guidance document as a tool to help in compliance efforts. The first column of this summary chart is taken verbatim from the guidance document. The middle column is the checklist of requirements that our council distilled from the main body of the guidance and the final column can be used by organizations to document evidence of compliance.

A: Building Blocks: Organizational Commitment & Program Controls

Privacy Management Program – At a Glance	Checklist of Privacy Regulatory Authority Expectations	Documentation/ Evidence of Compliance
Organizational Commitment		
General Requirements	• The organization has developed an internal governance structure that fosters a privacy respectful culture • The internal governance structure includes privacy-related processes • The internal governance structure includes means to ensure that privacy-related processes are being followed *(see Page 6)*	
Buy-In from the Top • Senior Management support is key to a successful privacy management program and essential for a privacy respectful culture	• Senior management supports/champions the privacy management program • Senior management provides the resources that the privacy management program needs to succeed • Senior management has appointed a privacy point person ("Privacy Officer") • Senior management endorses the privacy program controls • Senior management monitors, and reports to the Board of Directors as appropriate on, the privacy management program *(see Pages 6-7)*	
Privacy Officer • Role exists and is fundamental to business decision-making process • Role and responsibilities for monitoring compliance are clearly identified and communicated throughout the organization • Responsible for the development and implementation of the program controls and their ongoing assessment and revision.	• The Privacy Officer is responsible for the privacy management program and compliance with applicable privacy legislation The Privacy Officer's duties include: • Establishing a privacy management program that demonstrates compliance by mapping the program to applicable legislation • Establishing and implementing program controls • Coordinating with other appropriate persons responsible for related disciplines and functions within the organization • Ongoing assessment and revision of program controls • Representing the organization in the event of a compliant investigation by privacy commissioner's office • Advocating privacy within the organization • Resources are dedicated to training the Privacy Officer *(see Page 7)*	

Privacy Office • Role is defined and resources are identified and adequate. • Organizational structure supports the ability of staff to monitor compliance and foster a culture of privacy within the organization • Ensures privacy protection is built into every major function involving the use of personal information.	• The Privacy Officer is supported by dedicated staff (in larger organizations) • The role of the Privacy Officer is defined • The Privacy Office's resources are identified and adequate • The organizational structure supports the ability of staff to monitor compliance • The organizational structure fosters a culture of privacy within the organization • The Privacy Office ensures privacy protection is built into every major function involving the use of personal information (e.g. product development, customer services, marketing) *(see Page 8)*	
Reporting • Reporting mechanisms need to be established, and they need to be reflected in the organization's program controls.	• There are privacy reporting mechanisms that ensure that the right people know how the privacy management program is structured and whether it is functioning as expected • Senior management and the Board of Directors receive reports on privacy • Reporting mechanisms are reflected in the organization's program controls • An internal audit and assurance program monitors compliance with privacy policies • An escalation procedure has been clearly defined and explained to all employees (e.g. for when there is a security breach or when a customer complains) • The escalation procedure is monitored to ensure necessary steps are being taken when triggered (e.g. test runs of privacy breach identification, escalation and containment protocols) The reporting program: • Clearly defines its reporting structure (in terms of reporting on its overall compliance activities) as well as employee reporting structures in the event of a complaint or potential breach • Tests and reports on the results of its internal reporting structures • Document all of its reporting structures *(see Pages 8-9)*	

Program Controls		
Personal Information Inventory • The organization is able to identify: the personal information in its custody or control, its authority for the collection, use and disclosure of the personal information, and the sensitivity of the information	• The organization has completed a personal information inventory or equivalent The personal information inventory is documented and the organization is able to identify: • The types of personal information that it holds and where it is held (including by third parties) • why/how it is collecting personal information • why it is using personal information • why/to whom it is disclosing personal information • The sensitivity and/or classification of the personal information *(see Pages 9-10)*	

Policies
 	
• Collection, use and disclosure of personal information, which include requirements for the consent and notification
• Access to and correction of personal information
• Retention and disposal of personal information
• Responsible use of information and information technology, including administrative, physical and technological security controls and role-based access
• Challenging compliance
	• Internal privacy policies have been documented and developed to address obligations under Canadian privacy legislation ("Privacy Policies")
	• Privacy Policies show how they are connected to Canadian privacy legislation
	• Privacy policies are available to employees
	• Privacy policies are periodically signed-off by employees
	• Privacy compliance requirements are incorporated in other policies, as appropriate (e.g. contract management, procurement and human resources policies)
	
	The following key policies are in place:
	
	• Collection, use and disclosure of personal information, including requirements for consent and notification
	  ○ Employees are made aware of their obligation to inform individuals of the reasons, and obtain their consent, for the collection, use and disclosure of personal information
	• Access to and correction of personal information
	  ○ Employees are made aware that individuals have a right to access and correct personal information
	  ○ Employees are made aware of how to help customers and employees exercise their right of access by knowing what processes to follow, including timelines in which the organization must respond
	• Retention and disposal of personal information
	• Responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls
	  ○ Access to information is limited based on an individual's role
	  ○ Employees have access to the minimum amount of	

	personal information they need to perform their duties within the organization ○ Roles are documented, remain up-to-date, and assigned on a consistent basis, preferably by a central authority within the organization • Challenging compliance (i.e. policy for staff to follow in the event that individuals wish to complain about the organization's personal information handling) *(see Pages 10-12)*	
Risk Assessment Tools	• Risk assessments are conducted, at least on an annual basis, to ensure compliance within applicable legislation • A risk assessment is conducted on new or modified projects involving personal information • A privacy risk assessment is conducted on any new collection, use or disclosure of personal information • There is process for identifying and mitigating privacy and security risks ○ This process includes the use of privacy impact assessments ○ This process includes the use of security threat risk assessments • There is a procedure for conducting privacy impact assessments • There is a procedure for conducting security threat risk assessments • There is a review and approval process that involves the Privacy Officer/Office when designing new initiatives, services or programs *(see Page 12)*	
Training and Education Requirements	• All members of the organization are aware of their privacy obligations • All members of the organization are ready to act on privacy obligations • Employees are required to undergo training and education, tailored to their specific needs ○ The employee training and education is recurrent ○ The content of the program is periodically revisited and updated to reflect changes • Employees are required to sign an agreement to comply with the organization's policies and program controls • The training processes are documented • Participation in training processes are measured • The success in the training processes is measured • Privacy training and education is mandatory for all new employees before they access personal information and periodically thereafter	

	• Privacy training and education covers the policies and procedures established by the organization • The training program allows for the circulation of essential information to relevant employees as soon as practical if an urgent need arises *(see Pages 12-14)*	
Breach and Incident Management Response Protocols	• There is a procedure for the management of personal information breaches • There is a person responsible for managing a breach • Responsibilities for internal and external reporting of the breach are defined *(see Page 14)*	
Service Provider Management	• There are contractual or other requirements in place with service providers to protect personal information • Trans-border data flows and requirements of the foreign regime are addressed in service provider arrangements, as appropriate • Sensitivity of personal information is addressed in service provider arrangements, as appropriate Privacy requirements for service providers include the following: • Compliance requirements, such as binding the service provider to the policies and protocols of the organization and requiring the organization to be notified in the event of a breach • Training and education for all service provider employees with access to personal information • Restrictions on sub-contracting • Audits • Agreements with service provider employees stating that they will comply with the organization's privacy policies and protocols *(see Pages 14-15)*	
External Communication	• There is a procedure for informing individual of their privacy rights • There is a procedure for informing individuals of the program controls • The external communication is clear and understandable and not simply a reiteration of the law External communication: • Provides enough information so that individuals know the purpose of the collection, use and disclosure of personal	

	information as well as how it is safeguarded and how long it is retained • Notifies individuals if their personal information is being transferred outside of Canada • Includes information on who to contact with questions or concerns about the management of personal information • Is easily made available to individuals • Individuals are made aware of their ability to access their personal information held by the organization • Individuals are made aware of how to request a correction or complain about the organization's privacy compliance, including the right to challenge the organization's actions by submitting a complaint to the Privacy Commissioner *(see Page 15)*	

B: Ongoing Assessment & Revision

Develop an Oversight and Review Plan • Privacy Officer should develop an oversight and review plan on an annual basis that sets out how s/he will monitor and assess the effectiveness of the organization's program controls.	• The Privacy Officer develops an oversight and review plan on an annual basis that sets out how the privacy management program's effectiveness will be monitored and assessed • The plan establishes performance measures • The plan includes a schedule of when all policies and other program controls will be reviewed	
Assess & Revise Program Controls		
General Requirements	• The effectiveness of program controls are monitored, periodically audited and revised, where necessary The monitoring addresses the following: ○ The latest threats and risks ○ Whether program controls are addressing new threats ○ Whether program controls are reflecting the latest complaint, audit findings or guidance of the privacy commissioners ○ Whether new services being offered involve increased collection, use or disclosure of personal information ○ Whether training is occurring and if it is effective ○ Whether policies and procedures are being followed ○ Whether the privacy management program is up to date	

	• Problems identified during monitoring are documented and addressed • The Privacy Officer conducts periodic assessments to ensure key processes are being respected • The organization has developed metrics to gauge progress with respect to compliance • Assessments of program controls are conducted in a focused, continuous and thorough manner *(see Pages 16-17)*	
Update Personal Information Inventory	• A personal information inventory is kept current • New collections of personal information are identified and evaluated • New uses of personal information are identified and evaluated • New disclosures of personal information are identified and evaluated *(see Page 17)*	
Revise Policies	• Policies are reviewed and revised, as needed, following assessments or audits, in response to a breach or complaint, new guidance, industry based best practices, or as a result of environmental scans *(see Page 18)*	
Treat Risk Assessment Tools as Evergreen	• Privacy impact assessments are treated as evergreen documents so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed • Security threat and risk assessments are treaed as evergreen documents so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed *(see Page 18)*	
Modified Training and Education	• Training and education programs are reviewed and modified on a periodic basis as a result of ongoing assessments • Changes to program controls are effectively communicated to employees as they are made, or in “refreshed” education and training modules *(see Page 18)*	
Adapt Breach and Incident Response Protocols	• Breach and incident management response protocols are reviewed and revised to implement best practices or recommendations • The breach and incident response protocol is reviewed and revised to implement lessons learned from post-incident	

	reviews *(see Page 18)*	
Fine-Tune Service Provider Management	• Contracts with service providers are reviewed and, where necessary, fine-tuned *(see Page 18)*	
Improve External Communication	• External communications explaining privacy policies are reviewed, updated and clarified, as needed *(see Page 18)*	