Office of the Information and Privacy Commissioner of Alberta

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Getting Accountability Right with a Privacy Management Program

Purpose

The Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia have worked together to develop this document with the goal of providing consistent guidance on what it means to be an accountable organization. It is intended for organizations subject to our respective private-sector privacy legislation and outlines what we expect to see in a privacy management program.

What is accountability?

Accountability in relation to privacy is the acceptance of responsibility for personal information protection. An accountable organization must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws. Done properly, it should promote trust and confidence on the part of consumers, and thereby enhance competitive and reputational advantages for organizations.

The concept of accountability appears straightforward, but constructing a privacy management program within an organization takes careful planning and consideration across disciplines and job functions. Employees of accountable organizations should be aware of and understand the applicable parts of the organization's privacy management program. Customers, partners, and service providers should likewise be made aware of and given confidence in relevant aspects of the privacy management program. Finally, accountable organizations should be able to demonstrate to Privacy Commissioners that they have an effective, up-to-date privacy management program in place in the event of a complaint investigation or audit. They will want to ensure that they are correctly identifying privacy-related obligations and risks and appropriately taking them into account in developing their business models and related technologies and business practices before they launch new products or services. They will want to

minimize risks to their organization and to their employees and customers, as well as mitigate the effects of any privacy breaches.

There will be times when mistakes are made. However, with a solid privacy management program, organizations will be able to identify their weaknesses, strengthen their good practices, demonstrate due diligence, and potentially raise the protection of personal information that they hold to a higher level than the bare minimum needed to meet legislative requirements.

This document outlines what we think are the best approaches for developing a sound privacy management program, for organizations of all sizes, in order to meet obligations under applicable privacy legislation.

This document is not a "one-size-fits-all" solution, however. Each organization will need to determine, taking into consideration its size, how best to apply the guidance found here to develop a privacy management program. Public sector and health-care institutions will also find this document useful in establishing their own privacy management programs.

Part A of this document outlines "building blocks" or baseline fundamentals that every organization needs to have. Elements such as organizational commitment and program controls are essential.

Part B discusses how to maintain and improve a privacy management program on an ongoing basis.

A privacy management program should never be considered a finished product; it requires ongoing assessment and revision in order to be effective and relevant. The building blocks must be monitored and assessed on a regular basis and be updated accordingly.

The end result is that the building blocks are always evolving to keep pace with changes both within and outside the organization. This could encompass changes in such areas as technology, business models, law and best practices.

The Canadian Context

There are four statutory privacy regimes that may apply to the private sector in Canada. The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to federal works, undertakings or businesses (and to their employee personal information), and to provincially regulated businesses in provinces without substantially similar privacy legislation that collect, use or disclose personal information in the course

of commercial activities.[1] Three provinces have enacted private sector privacy laws which have been deemed by the Government of Canada to be "substantially similar" to PIPEDA – British Columbia, Alberta and Quebec.[2] British Columbia and Alberta have enacted *Personal Information Protection Acts* and Quebec has an *Act Respecting the Protection of Personal Information in the Private Sector*. [3]

The accountability principle is the first of 10 fair information principles under Schedule 1 of PIPEDA and is implicit in Alberta, British Columbia and Quebec's respective laws. It is the first among the principles because it is the means by which organizations are expected to give life to the rest of the fair information principles that are designed to appropriately handle and protect the personal information of individuals. (The full text of the accountability principle in Schedule 1 of PIPEDA is attached as **Appendix A**.)

International Context

The joint, federal-provincial nature of this guidance document is important given that personal information has become a global commodity, flowing constantly around the world, touched by organizations operating in multiple jurisdictions. The need for consistent approaches to personal information protection has never been greater.

Indeed, the global nature and the vast quantities of personal information flows have caused many privacy experts to examine in closer detail what it means for an organization to be accountable for protecting personal information. It has also caused experts to reflect further on how the concept of accountability can be leveraged to drive home the importance of protecting personal information in organizations in jurisdictions that may not have privacy legislation.

The accountability principle was first expressed in the Organisation for Economic Co-operation and Development's (OECD) 1980 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, the first internationally agreed-to set of privacy principles. PIPEDA encompasses the Canadian Standards Association (CSA) Model Code (found in Schedule I of the Act), which was highly influenced by the OECD Guidelines. Since then, the accountability principle has been included in the Asia-Pacific Economic Cooperation's (APEC) Privacy Framework. Cross-border privacy

[1] PIPEDA, s. 26(2)(b)
[2] Organizations in the Province of British Columbia Exemption Order, SOR/2004-220; Organizations in the Province of Alberta Exemption Order, SOR/2004-219; Organizations in the Province of Quebec Exemption Order, SOR/2003-374.
[3] Three provincial statutes (in Ontario, New Brunswick and Newfoundland and Labrador) that regulate the handling of personal health information have substantially similar status.

rules are being developed within that region to implement the APEC Privacy Framework. These rules will elaborate on the principle of accountability.

The concept of accountability is also gaining interest within the European Union. The Article 29 Working Party Opinion on Accountability contains a thoughtful analysis of what accountability in privacy means and what might be expected of organizations in the future in demonstrating compliance, and puts forward a proposal that it believes should help "data protection move from 'theory to practice' as well as helping data protection authorities in their supervision and enforcement tasks." The European Commission has proposed a new European Union legal framework for privacy that contains a provision concerning accountability. Under it, organizations would be required to adopt policies and implement appropriate procedures to demonstrate that their processing of personal data is compliant with the proposed Regulation.

Apart from international agreements and domestic privacy law, Safe Harbor, self-certification programs, and Binding Corporate Rules are all examples of the use of the concept of accountability to promote privacy protection while supporting transborder data flows. The Accountability Project, an initiative led by the US-based Centre for Policy and Information Leadership, with participation from representatives of data protection authorities, business and academia, is examining what it means for an organization to be "accountable" for its privacy practices. The OPC and British Columbia Information and Privacy Commissioner have participated in this international initiative.

The benefits of implementing a privacy management program

Every organization that is subject to Canada's private-sector privacy laws is obliged to be in compliance with them. A comprehensive privacy management program provides an effective way for organizations to satisfy regulators and assure themselves that they are compliant. But it is more than that.

Such a program helps foster a culture of privacy throughout an organization. Senior management support is vital to achieving this goal. When senior management provides the needed resources to ensure appropriate training and education, risk assessment and monitoring, and auditing, it sends a clear signal that privacy is vital to the organization. In turn, a culture of privacy encourages employee support and reinforces the privacy protections the organization puts in place. When an organization takes the position that privacy is vital to its operations and "walks the talk" by implementing a robust privacy management program, enhanced trust that is essential for customers and clients to engage with that organization follows. An organization that has a strong privacy management program may enjoy an enhanced reputation that gives it a

competitive edge. In the longer term, a privacy management program that is scaled to the organization's needs will save money and make good business sense.

Conversely, without strong privacy protection, trust will erode to an organization's detriment. For example, privacy breaches are expensive for organizations – both in terms of "clean up" and reputation repair. Breaches may also prove expensive for the affected individuals. An appropriately designed and implemented privacy management program may help minimize the risk of such breaches, maximize the organization's ability to identify and address such incidents, and minimize their damage.

Given the vast amounts of personal information held by organizations and institutions, the increasing economic value of this information, and the heightened attention and concern regarding privacy breaches, it is vital that organizations take steps to develop and strengthen their privacy management programs to minimize risks and increase compliance.

Canadians expect and deserve it.

Part A Building Blocks

Accountability fundamentals: Developing a Comprehensive Privacy Management Program

What should an organization do to ensure that it is handling personal information appropriately? How will it know that it is doing it right? How will it be able to demonstrate to itself, its clients and to privacy commissioners that it has the capacity to comply and has complied with its legal obligations?

Accountability has a number of important requirements. Organizations are required to appoint someone to oversee the development, implementation and maintenance of the organization's privacy protection program. Policies and processes are needed, and training of employees required. Contracts (or other means) are required when organizations transfer personal information to third parties for processing, to ensure that the information in question is protected in a manner that is comparable to how the organization would protect it. Organizations are expected to have systems in place to respond to requests from individuals for access to (and correction of) their personal information, and they need to be able to respond to complaints from individuals about how personal information is being protected.

The OPC has developed a number of tools that will be of use to organizations to learn the basics about privacy and privacy legislation. These include: *Your Privacy*

Responsibilities: A Guide for Businesses and Organizations; *Privacy Questionnaire: Is Your Business Ready*? and a video for small- and medium-sized organizations entitled *PIPEDA for Business: What you need to know about protecting your customers' privacy*.

Alberta has developed the following documents which will be of assistance: *Guide for Businesses and Organizations on the Personal Information Protection Act*; *Information Privacy Rights*; and *10 Steps to Implement PIPA*.

British Columbia has also developed similar tools relating to BC's private sector legislation including:
A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations

Part A will outline the building blocks that are essential components of a privacy management program that is demonstrably compliant with Canada's applicable private-sector privacy legislation.

1. Organizational commitment

This first building block is the development of an internal governance structure that fosters a privacy respectful culture.

Organizations are expected to develop and implement program controls that give effect to the privacy principles contained in the Federal, Alberta, and British Columbia private-sector privacy laws. Compliance with the laws, however, requires organizations to have a governance structure in place, with processes to follow and the means to ensure that they are being followed. Fundamentally, in order to be compliant and effective, a privacy-respectful culture needs to be cultivated.

a) Buy-in from the top

Senior management support is key to a successful privacy management program and essential for a privacy respectful culture.

When senior management is committed to ensuring that the organization is compliant with privacy legislation, the program will have a better chance of success, and a culture of privacy will more likely be established.

Senior management needs to actively champion the privacy program. It should:

- appoint the privacy point person(s) (Privacy Officer);
- endorse the program controls; and
- monitor and report to the Board, as appropriate, on the program.

Senior management will also need to provide support for the resources the program needs to succeed.

b) Privacy Officer

Organizations must appoint someone who is responsible for the privacy management program.

Whether this person is a C-level executive of a major corporation or the owner/operator of a very small organization, someone must be assigned responsibility for overseeing the organization's compliance with applicable privacy legislation. Other individuals may be involved in handling personal information, but the Privacy Officer is the one accountable for structuring, designing and managing the program, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up. Organizations should expect to dedicate some resources to training the Privacy Officer. The Privacy Officer should establish a program that demonstrates compliance by mapping the program to applicable legislation. It will be important to show how the program is being managed throughout the organization.

The Privacy Officer will play many roles with respect to privacy. S/he will:

- establish and implement program controls;
- coordinate with other appropriate persons responsible for related disciplines and functions within the organization;
- be responsible for the ongoing assessment and revision of program controls;
- represent the organization in the event of a complaint investigation by a privacy commissioner's office; and
- advocate privacy within the organization itself.

This last role is as crucial as the others. Organizations face competing interests and privacy compliance is one program of many. Privacy, however, is more than a balancing of interests. Privacy should be seen in terms of improving processes, customer relationship management, and reputation. Consequently, the privacy management program's importance must be recognized at all levels.

It should be noted that an organization remains accountable for compliance with applicable privacy legislation. Appointing an individual to be responsible for the program does not negate the organization's accountability[4].

c) Privacy Office

For larger organizations, staff assigned to work on privacy issues will be needed.

[4] http://www.priv.gc.ca/cf-dc/2001/cf-dc_011204_e.asp

In larger organizations, the Privacy Officer will need to be supported by dedicated staff. The role of the Privacy Office must be defined and its resources must be identified and adequate. Staff of the Privacy Office should have delegated responsibilities to monitor compliance and foster a culture of privacy within the organization. The Office should also work to ensure that privacy protection is built into every major function involving the use of personal information, including product development, customer services or marketing initiatives.

d) Reporting

Reporting mechanisms need to be established, and reflected in the organization's program controls.

The organization needs to establish internal reporting mechanisms to ensure that the right people know how the privacy management program is structured and whether it is functioning as expected. Within fairly large organizations, the audience for this information is likely to be senior management, and in turn, senior management reports to the board of directors. All reporting mechanisms should be reflected in the organization's program controls.

Organizations should establish some form of internal audit and assurance programs to monitor compliance with their privacy policies. This could include the form of customer and employee feedback for smaller organizations, or for some larger organizations, third-party verifications. These reports will also help should the organization be subject to an investigation or audit under applicable privacy legislation as they are likely to demonstrate due diligence.

However, there is more to reporting than this. There will be times when privacy issues need to be escalated, for example, when there is a security breach or when a customer complains. Escalation means both involving people of relevant responsibility and ensuring that all the needed persons in the organization are included in the resolution of the issue. In large organizations, this could include, for example, representatives from technical, legal and corporate communications. How and when to escalate must be clearly defined and explained to all employees. To ensure that related processes are being followed, organizations will need to monitor whether the needed steps are being taken when triggered. Some organizations have found it useful to conduct test runs of their privacy breach identification, escalation and containment protocols, for example.

An effective 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 a potential breach;

- tests and reports on the results of its internal reporting structures; and
- documents all of its reporting structures.

2. Program controls

Program controls form the second building block. These help ensure that what is mandated in the governance structure is implemented in the organization. This section identifies the program controls in a privacy management program. Developing these controls will assist the Privacy Officer in structuring an appropriate privacy management program within the organization and the controls will be used to demonstrate how the program is compliant with privacy legislation.

a) Personal Information Inventory

Whether it has a sophisticated privacy management program in place or is implementing a new one, every organization can benefit from carefully examining the personal information it holds and how it currently handles this information.

An organization needs to know what personal information it holds, how it is being used – and whether it really needs it at all. Understanding and documenting the types of personal information that an organization collects and where it is held are critically important. This will affect the type of consent the organization obtains from individuals and how the information is protected; and it will make it easier to assist individuals in exercising their access and correction rights. Every component of an accountable, compliant privacy management program begins with this assessment.

Determining what is or is not personal information is not always a simple task, however. The OPC has issued an Interpretation on the definition of personal information, which organizations may find useful. It summarizes various court decisions and OPC findings on the definition. Whether sensitive (such as financial or health information) or not, all personal information must be appropriately safeguarded and only used for the purpose(s) for which it was collected. Sensitive information may require special treatment[5].

Every organization needs to determine:

- what personal information it holds and where it is held (within the organization or by third parties , for example) and document this assessment;

[5] Some personal information is almost always considered sensitive, such as financial or health information. Other personal information may be considered sensitive, depending on the context. Sensitive personal information may require greater safeguards and express consent.

- why it is collecting, using or disclosing personal information and document these reasons; and
- the sensitivity of the personal information it holds.

A document entitled *Securing personal information: a self-assessment tool for public bodies and organizations*, issued by our Offices, also covers issues related to taking stock of personal information.

b) Policies

Organizations must develop and document internal policies that address obligations under the law. These policies need to be available to employees, and employees need to periodically sign off on them.

Organizations are required to develop internal policies that give effect to the principles contained in Canadian private-sector privacy legislation. These policies should be documented and should show how they connect to the applicable privacy legislation.

The key policies that organizations must have in place are the following:

i. Collection, use and disclosure of personal information, including requirements for consent and notification;
ii. Access to and correction of personal information;
iii. Retention and disposal of personal information;
iv. Responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls;
v. Challenging compliance.

Organizations should also incorporate privacy compliance requirements in other policies of the organization as appropriate. For example, in contract management policies, procurement policies, human resources policies and policies dealing with the disclosure of personal information to regulatory bodies, law enforcement agencies and internal security departments.

Organizations are required to develop internal policies that give effect to the principles contained in Canadian private-sector privacy legislation.

Each of the key policies is discussed below.

i. Collection, use and disclosure of personal information, which include requirements for consent and notification

It is important that employees understand their obligation to inform individuals of the reasons, and obtain their consent, for the collection, use and disclosure of personal

information. Privacy legislation requires that personal information only be collected, used or disclosed for appropriate purposes and limited to those purposes.

ii. Access to and correction of personal information

Employees need to understand that individuals have a right to access and correct personal information. Employees should understand how to help customers and employees exercise this right by knowing what processes to follow, including the timelines in which the organization must respond.

iii. Retention and disposal of personal information

In order to minimize unauthorized collection, use and disclosures, organizations should not retain personal information that is no longer required for the delivery of their services. Organizations must also have a policy regarding the disposal or destruction of records. Customers have the expectation that an organization will dispose of their personal information when it is no longer needed. As such, organizations should securely dispose of customers' records in accordance with its policy.

iv. Responsible use of information and information technology, including administrative, physical and technological security controls and role-based access

Organizations must protect the personal information they hold by making reasonable security arrangements. What is reasonable depends on the sensitivity of the information. For example, security arrangements could include locked filing cabinets, access controls and encryption to protect electronic databases. It is a very significant responsibility and, in most instances, requires specialized technical expertise to design an appropriate system.

Role-based access control is one of the best ways for organizations to limit who has access to what information. In accordance with "need to know" principles, employees should only have access to the minimum amount of personal information they need to perform their duties within the organization. Roles must be documented, remain up-to-date and assigned on a consistent basis, preferably by a central authority within the organization.

All three laws require that safeguards be in place to protect personal information.

The OPC, Alberta and British Columbia OIPCs have produced a document on securing personal information that is intended to help organizations, particularly small- and medium-sized enterprises, think about various aspects of their operations that may have

an impact on the security of personal information. We recommend that organizations review this tool.

v. Challenging compliance

Individuals have the right to challenge an organization's compliance with applicable privacy legislation. Organizations should therefore have internal policies in place for staff to follow in the event that individuals wish to complain about the organization's personal information handling practices.

c) Risk assessment tools

Privacy risks evolve over time. Conducting risk assessments, at least on an annual basis, is an important part of any privacy management program to ensure that organizations are in compliance with applicable legislation.

We have seen instances of organizations offering new services that collect, use or disclose personal information that have not been thoroughly vetted from a privacy perspective. Proper use of risk assessment tools can help prevent problems. Fixing a privacy problem after the fact can be costly so careful consideration of the purposes for a particular initiative, product or service, and an assessment that minimizes any privacy impacts beforehand is vital.

As a result, such assessments should be required throughout the organization for all new[6] projects involving personal information and on any new collection, use or disclosure of personal information. Organizations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk assessments.

Organizations should develop procedures for conducting such assessments, and develop a review and approval process that involves the Privacy Officer/Office when designing new initiatives, services or programs. For larger organizations, the Privacy Officer should be aware of the review process, and where there are high-risk initiatives, services or programs, the Privacy Office should be directly involved.

d) Training and education requirements

A sound privacy management program requires all members of an organization to be aware of, and be ready to act on privacy obligations. Up-to-date training

[6] A new project may be modifying existing systems, components and processes.

and education requirements for all employees, tailored to specific needs, are key to compliance.

In order for a privacy management program to be effective, employees must be actively engaged in privacy protection. They need to be educated in privacy protection generally, and for those who handle personal information directly, they will need additional training specifically tailored to their roles. Training and education need to be recurrent, and the content of the program needs to be periodically revisited and updated to reflect changes.

Training and general education on privacy are very important. Our Offices have seen instances where issues were not identified as privacy issues when they should have been. As a result, appropriate steps were not taken to prevent or address privacy breaches.[7] In other cases, we have seen a lack of awareness or appreciation for privacy risks on the part of employees result in the development of products or services that were not compliant with applicable privacy law.[8] In Alberta, human error is the most common cause of reported breaches resulting in a real risk of significant harm to an individual. Examples include: misdirected faxes and mail, e-mail addresses viewable in mass e-mails, inappropriate disposal of documents, and disclosure of passwords.

Employees will be able to better protect privacy when they are able to recognize a matter as one that involves personal information protection. Organizations may have very sound policies and program controls in place but if employees do not follow them, the privacy management program has broken down. Employees should be required to sign an agreement to comply with the organization's policies and program controls.

There are numerous ways for organizations to deliver training and general privacy education. Examples include, providing mandatory training modules on the company intranet, small group sessions, one-on-one training, monthly e-newsletters, or inserting modules within training on organization policies. The organization should document its training processes and measure participation and success.

For privacy training and education to be effective, it must:

- be mandatory for all new employees before they access personal information and periodically thereafter;
- cover the policies and procedures established by the organization;
- be delivered in the most appropriate and effective manner, based on organizational needs; and

[7] For an example, see http://www.priv.gc.ca/cf-dc/incidents/2005/050418_01_e.asp.
[8] For an example, see http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_e.asp, involving Google's collection of personal information from unencrypted wifi networks.

- circulate essential information to relevant employees as soon as practical if an urgent need arises.

e) Breach and incident management response protocols

Risk assessments, both internal and external, may help mitigate privacy breaches, which are unfortunately becoming a frequent fixture in the news. As previously noted, breaches are expensive on many fronts and taxing on consumer trust.

As a result, organizations should have a procedure in place and a person responsible for managing a personal information breach. For larger organizations, a collaborative approach may be required, with employees from different parts of the organization working together. Responsibilities for internal and external reporting of the breach must be clear.

In Alberta, an organization that has personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

Reporting to privacy commissioners and notification of affected individuals may also be required. Organizations operating in Alberta or collecting personal information of Alberta residents are required by law to report certain breaches to the Information and Privacy Commissioner of Alberta. Regardless of whether reporting is mandatory or not in a particular jurisdiction, organizations are encouraged to report breaches to the appropriate offices.

For more guidance on the expectations regarding breaches, please see BC's *Privacy reach checklist for private organizations* and *Privacy breaches: tools and resources for the private sector*; Alberta's *Reporting a Breach to the Commissioner*; *Breach Report Form*; *Notifying Affected Individuals*; and the OPC's *Privacy Breach Handbook*.

f) Service provider management

Personal information handling by third parties is another key area to consider. Are there contractual or other means in place to protect that personal information? Is the information leaving the country? If so, has the organization taken into consideration the sensitivity of the information and the requirements of the foreign regime? The OPC's *Guidelines for Processing Personal Data Across Borders* provides additional information on accountability and the use of third-party processors and trans-border data flows.

Such considerations are part of assessing risk. At a minimum, privacy requirements for service providers should include the following:

- privacy provisions in contracts setting out requirements for compliance including 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;
- sub-contracting;
- audits; and agreements with service provider employees stating that they will comply with the organization's privacy policies and protocols.

The law stipulates that the organization that is transferring personal information to a third party for processing remains responsible for the personal information. Contractual or other means may be used to provide protection; policies and procedures may need to include information on where the information is going and why.

g) External communication

Organizations also have to develop a procedure for informing individuals of their privacy rights and the organization's program controls. This external communication should be clear and understandable and not simply a reiteration of the law. It should:

- provide enough information so that the public knows the purpose of the collection, use and disclosure of personal information as well as how it is safeguarded and how long it is retained;
- notify individuals if their personal information is being transferred outside of Canada;
- include information on who to contact with questions or concerns; and
- be made easily available to individuals.

Individuals should be made aware of their ability to access their personal information held by the organization, and how to request correction or to complain about the organization's privacy compliance, including the right to challenge the organization's actions by submitting a complaint to the Privacy Commissioner.

The OPC has developed a number of documents that are useful for organizations developing internal policies and external communication. These include: *Build a Privacy Plan for your Business*; *PIPEDA Self-Assessment Tool*; *Privacy Guide for Small Businesses: The Basics*; *Guidelines for Processing Personal Data Across Borders*; *Privacy and Your Business: Privacy Breach Handbook*; and *Your Privacy Responsibilities: A Guide for Businesses and Organizations*.

Alberta has developed the following documents: *Key Steps in Responding to Privacy Breaches*; *PIPA Advisory 2: Access Requests: An Overview*; *PIPA Advisory 3: Access Requests: Responding to a Request*; and *PIPA Advisory 8: Access Requests: Reasonable Safeguards*.

British Columbia's resources include: *Privacy breach checklist for private organizations;* *Privacy breaches: tools and resources for the private sector*.

Part B Ongoing Assessment and Revision

Part A describes the building blocks of creating a privacy management program. Part B of this document outlines the critical tasks involved in the maintenance of a privacy management program to ensure ongoing effectiveness, compliance and accountability. In order to properly protect privacy and meet legal obligations, organizations must monitor, assess and revise their framework to ensure it remains relevant and effective. In order to accomplish this work, sufficient resources and training must be allocated to the Privacy Officer.

1. Develop an Oversight and Review Plan

An oversight and review plan will help the organization keep its privacy management program on track and up to date.

The Privacy Officer should develop an oversight and review plan on an annual basis that sets out how and when s/he will monitor and assess the organization's privacy management program's effectiveness, as outlined in organizational commitments. The plan should establish performance measures and include a schedule of when all policies and other program controls will be reviewed.

2. Assess and Revise Program Controls

The effectiveness of program controls should be monitored, periodically audited, and where necessary, revised.

Monitoring is an ongoing process and should address at a minimum the following questions:

- what are the latest threats and risks?

- are the program controls addressing new threats and reflecting the latest complaint or audit findings, or guidance of the privacy commissioners?
- are new services being offered that involve increased collection, use or disclosure of personal information?
- is training occurring, is it effective, are policies and procedures being followed, and is the program up to date?

If there are problems found during the monitoring process, concerns will need to be documented and addressed by the appropriate officials.

For critical or high-risk processes, periodic internal or external audits are important ways to assess the effectiveness of an organization's privacy program. However, at a bare minimum, the Privacy Officer should conduct periodic assessments to ensure key processes are being respected. For smaller organizations or for less formal reviews, organizations should develop checklists that are reviewed on a regular basis. Through whatever means appropriate,, organizations need to ensure that employees or contractors are following the organization's policies and program controls.

As noted earlier, this document is not a "one-size-fits-all" solution. Each organization will need to decide how to structure its own privacy management program, taking into consideration a number of factors, including the size of the organization, and the amount and sensitivity of the personal information it handles.

When organizations begin developing their privacy management programs, they may not have in place every element of a compliant program. Even organizations with fairly mature programs need to ensure that they are taking reasonable steps to maintain compliance. It is important for any organization to gauge progress through the use of metrics, with continued compliance being the objective.

The expectation is that an organization conducts assessments of its program controls (as outlined in Part A) in a focused, continuous and thorough manner.

Based on the results of the assessment process, the Privacy Officer must consider whether to take action to update and revise the program controls. This is a critical responsibility. The changes must be communicated to employees either as they are made or in "refresher" education and training modules.

In short, the following actions will need to be undertaken by the Privacy Officer:

a) **monitor and update personal information inventory** continuously to keep it current and identify and evaluate new collections, uses and disclosures;

b) **review and revise policies** 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. The importance of this work cannot be overstated. There is no point in having policies if they are not effective and relevant – or if nobody within the organization knows about them.

c) **treat privacy impact assessments and security threat and risk assessments as evergreen documents** so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed.

d) **review and modify training and education** on a periodic basis as a result of ongoing assessments and communicate changes made to program controls.

e) **review and adapt breach and incident management response protocols** to implement best practices or recommendations and lessons learned from post-incident reviews.

f) **review and**, where necessary, **fine-tune** requirements in contracts with **service providers.**

g) **update and clarify external communication** explaining privacy policies.

Conclusion

Demonstrating Compliance

Accountable organizations are able to demonstrate that they have a comprehensive privacy management program in place.

This document outlines the elements and strategies of a privacy management program that can help organizations "get accountability right". With such a program, organizations will be able to demonstrate to customers, employees, partners, shareholders, and privacy commissioners that they have in place a robust privacy compliance program. They will be able to describe and document all of the elements outlined in this guidance document and show evidence of how they have implemented their program.

Should there be an investigation by a Privacy Commissioner's office regarding a complaint about a possible contravention of the law or an audit of your practices, an organization may be asked to show how it addresses the requirements of the applicable law. The Privacy Officer needs to have the program fully documented in the event of such an occurrence. During an investigation or audit, our Offices will expect that

organizations can demonstrate that they have an up-to-date, comprehensive privacy program in place. Evidence of an effective privacy management program assists Commissioners in determining whether or not the organization has reasonable safeguards in place, and has complied with the accountability requirements under applicable law.

Organizations that do not meet that expectation will find themselves faced with additional work to establish or update such a program.

Beyond the law – Why privacy should matter to business

Within an organization, privacy is essential to establishing and maintaining trust. If customers, clients or employees believe that their personal information will be handled respectfully, in an open and transparent manner, with strong, reasonable safeguards, and made accessible to them at their request, this fosters trust and a continued positive relationship can be expected. If customers are typically considered a business' greatest asset, then their personal information must be considered one as well. Organizations will want to build and protect their assets, and personal information, as an asset, is no different.

An accountable organization can demonstrate to customers, employees, shareholders, regulators, and competitors that it values privacy, not only for compliance reasons, but also because privacy makes good business sense. It is hoped that the guidance contained in this document will help all organizations achieve that goal.

Privacy Management Program - At A Glance

A. Building Blocks

Organizational Commitment	**a) Buy-in from the top**	Senior management support is key to a successful privacy management program and essential for a privacy respectful culture.
	b) 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.
	c) 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.
	d) Reporting	Reporting mechanisms need to be established, and they need to be reflected in the organization's program controls.
Program Controls	**a) 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 personal information.

	b) Policies	i. Collection, use and disclosure of personal information, which include requirements for consent and notification ii. Access to and correction of personal information iii. Retention and disposal of personal information iv. Responsible use of information and information technology, including administrative, physical and technological security controls and role-based access v. Challenging compliance
	c) Risk Assessment Tools **d) Training and education requirements** **e) Breach and incident management response protocols** **f) Service Provider management** **g) External communication**	

B. Ongoing Assessment and Revision

Oversight and Review Plan	**a) Develop an oversight and review plan**	Privacy Officer should develop an oversight and review plan on an annual basis that that sets out how s/he will monitor and assess the effectiveness of the organization's program controls.
Assess and Revise Program Controls As Necessary	**a) Update personal information inventory** **b) Revise policies** **c) Treat risk assessment tools as evergreen** **d) Modify training and education** **e) Adapt breach and incident response protocols** **f) Fine-tune service provider management** **g) Improve external communication**	

Appendix A

The accountability principle in Schedule 1 of PIPEDA reads as follows:

4.1 Principle 1 – Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organizations' compliance with the following principles.

4.1.1

Accountability for the organizations' compliance with the principles rests with the designated individuals(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individuals(s).

4.1.2

The identity of the individuals(s) designated by the organization to oversee the organizations' compliance with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(a) Implementing procedures to protect personal information;
(b) establishing procedures to receive and respond to complaints and inquiries;
(c) training employees on and communicating information about the organization's policies and practices; and
(d) developing information to explain the organization's policies and procedures.