Archived - Privacy Impact Assessment Policy

Tools & Resources

Effective date

This policy takes effect May 2, 2002.

Preface

Governments across Canada are committed to privacy and the protection of personal information used in the course of providing programs and services to the public. The federal government is subject to the *Privacy Act*. Most provincial and territorial governments are subject to similar privacy laws and policies that regulate the collection, use and disclosure of personal information. In addition, the *Personal Information Protection and Electronic Documents Act* and equivalent provincial legislation extend privacy protection to govern the manner in which personal information is managed by the private sector.

Government departments and agencies are implementing electronic service delivery to enhance the services they provide to Canadians. Privacy implications and risks may arise because of the intra-institutional, inter-institutional or cross-jurisdictional flow of personal information. Electronic service delivery may also involve the private sector. Privacy risks inherent in these activities need to be identified, assessed and resolved to ensure that all program and system improvements respect and strengthen privacy.

Public opinion surveys consistently demonstrate that Canadians are concerned about privacy when their personal information is being used in the context of electronic service delivery. They are often reluctant to send personal information over the Internet in order to engage in electronic transactions. There are a number of privacy risks associated with advances in technology. They include transaction monitoring, data mining, common directory services, data matching, the use of common personal identifiers and the risks of identity theft and unintended disclosures of personal information. The ultimate challenge is to assist Canadians in understanding how the government handles their personal information and to trust it to do so responsibly, regardless of the service delivery channel they choose to use.

The *Privacy Impact Assessment Policy* is one of several tools designed to meet this challenge. It is based on privacy principles common to all data protection régimes. These principles are enumerated in the "Code of Fair Information Practices" in the federal *Privacy Act* as well as in the ten privacy principles attached to the *Personal Information Protection and Electronic Documents Act*. There are differences between the federal and provincial and private sector codes that must be taken into account when collaborating on cross-jurisdictional initiatives. However, they are premised on the fundamental concept that individuals have a right, subject to the explicit provisions of other legislation, to control the collection, use and disclosure of their personal information.

Privacy Impact Assessments provide a framework to ensure that privacy is considered throughout the design or re-design of programs or services. The assessments will identify the extent to which proposals comply with all appropriate statutes. Assessments assist managers and decision-makers to avoid or mitigate privacy risks and promote fully informed policy, program and system design choices.

The conduct of Privacy Impact Assessments is a shared management responsibility. They are co-operative endeavours requiring a variety of skill sets, including those of program managers, technical specialists and privacy and legal advisors. The deputy head of a federal institution, department or agency is accountable for determining if a PIA is required.

It is important to note that the assessment process is not intended for the development of new legislation. It is intended to be adapted to suit particular institutional program and service requirements. The *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks* are attached to the policy to assist institutions in conducting assessments. They are tools that institutions may adapt to assist them in assessing privacy issues. The process is also intended to be an iterative one that is maintained throughout the life cycle of programs or services as they are altered or re-designed.

The end result of the Privacy Impact Assessment is assurance that all privacy issues have been identified and resolved or mitigated. The associated documentation forms the basis for seeking the advice of and notifying the Privacy Commissioner as well as for assuring the public that privacy issueshave been addressed.

Policy objective

To assure Canadians that privacy principles are being taken into account when there are proposals for, and during the design, implementation and evolution of programs and services that raise privacy issues by:

- prescribing the development and maintenance of Privacy Impact Assessments; and
- outinely communicating the results of Privacy Impact Assessments to the Privacy Commissioner and the public.

Policy statements

The Government of Canada is committed to protecting the personal information of Canadians. Privacy, in conjunction with other relevant legislative and policy considerations, is integral to the design, implementation and evolution of all programs and services. Although often associated with electronic service delivery, Privacy Impact Assessments provide a consistent framework to determine privacy risks inherent in any service delivery channel, including in-person, mail, telephone and on-line services.

Institutions are responsible for demonstrating that their collection, use and disclosure of personal information respect the *Privacy Act* and privacy principles throughout the initiation, analysis, design, development, implementation and post-implementation review phases of their program and service delivery activities.

Institutions are also responsible for communicating with Canadians why their personal information is being collected and how it will be used and disclosed. They must explain the impact of new modes of program and service delivery on privacy and how associated issues will be resolved. The result will be that Canadians can make informed choices regarding the type of service delivery channel they wish to rely on in their relations with the federal government and will be assured that their privacy is being protected regardless of the channel they choose.

Therefore, it is the policy of the government to:

- ensure that privacy protection is a core consideration in the initial framing of program or service objectives and in all subsequent activities;
- ensure that accountability for privacy issues is clearly incorporated into the duties of program managers and any other participants, including those from other institutions, jurisdictions and sectors;
- provide decision-makers with the information necessary to make fully-informed policy, program, system design and procurement decisions based on an understanding of the privacy implications and risks and the options available for avoiding and/or mitigating those risks;
- reduce the risk of having to terminate or substantially modify a program or service after its implementation to comply with privacy requirements;
- provide documentation on the business processes and flow of personal information for use and review by departmental and agency staff and to serve as the basis for consultations with clients, the Privacy Commissioner and other stakeholders; and
- promote an awareness of sound privacy practices associated with program and service delivery by informing the Privacy Commissioner and the public of all proposals for new or modified programs and services that raise privacy issues.

Application

This policy applies to all government institutions listed in the Schedule to the *Privacy Act*, except the Bank of Canada.

Policy requirements

1. Legislation and policies

Institutions must develop and maintain Privacy Impact Assessments to evaluate whether program and service delivery initiatives involving the collection, use or disclosure of personal information comply with privacy requirements and to resolve privacy issues that may be of potential public concern. The *Privacy Act*, the *Privacy and Data Protection Policy*, the *National Archives of Canada Act*, program-specific legislation and regulationprovide an information management régime for the protection of personal information used by the government.

The Privacy Impact Assessment process is intended to be adapted to potential privacy implications associated with specific situations. Institutions must examine their own program legislation, regulation and policies to determine specific or additional privacy, information management and other requirements governing the personal information under their control. The examination must be conducted in consultation with the institutions' privacy policy and legal advisors. It should clarify the relationship between personal information and other types of information, such as business confidential information, and assist in determining the level of protection required.

Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks are attached as an Annex to this policy. The guidelines, which may be adapted by institutions, provide a step-by-step approach to the assessment process. Where programs and services involve cross-jurisdictional or cross-sectoral activities, they will assist institutions in identifying the requirements of the various legislations and ensure that the provisions of federal legislation and policies are respected.

2. Project initiation

Departments and agencies must conduct Privacy Impact Assessments for proposals for all new programs and services that raise privacy issues. For programs and services implemented prior to this policy, institutions must undertake assessments if they are substantially re-designing them or their delivery channels or transforming them for electronic service delivery in a manner that affects the collection, use or disclosure of personal information. Institutions may consider developing Privacy Impact Assessments for existing programs and services for which no changes are proposed if no previous assessments exist or if there are outstanding privacy issues.

Where applicable, institutions should consider the development of generic assessments. Generic assessments would be appropriate in instances where programs and services use the same or similar approaches to the collection, use and disclosure of personal information.

Institutions must initiate and define the scope of the Privacy Impact Assessments in the early stages of the design or re-design of a program or service so as to influence the developmental process. If the proposal involves:

- a new or increased collection, use or disclosure of personal information, with or without the consent of individuals;
- a broadening of target populations;
- a shift from direct to indirect collection of personal information;
- an expansion of personal information collection for purposes of program integration, program administration or program eligibility;
- new data matching or increased sharing of personal information between programs or across institutions, jurisdictions or sectors;
- development of or a new or extended use of common personal identifiers;
- significant changes to the business processes or systems that affect the physical or logical separation of personal information or the security mechanisms used to manage and control access to personal information; or
- the contracting out or devolution of a program or service to another level of government or the private sector;

A Privacy Impact Assessment is required. Detailed criteria to assist in determining when to conduct an assessment are contained in the *Privacy Impact Assessment Guidelines*.

At the initiation stage of a program or service, institutional officials should determine if a Preliminary Privacy Impact Assessment is warranted. They may develop a preliminary assessment, if they do not yet have the detailed information required for a comprehensive assessment, as a means of:

- identifying the types and volumes of personal information that are to be collected, used and disclosed;
- verifying the legislative and policy authorities for the proposed program or service;
- clarifying the roles, responsibilities and legal and policy status of the primary stakeholders, including those of other jurisdictions and the private sector;

- determining which aspects of the program or service are likely to involve privacy risks;
- initiating the consultation process with the Office of the Privacy Commissioner; and
- defining the scope of and the schedule for the final assessment.

The assessment tool is flexible and adaptable to initiatives ranging in scope from simple to complex. It is intended to avoid unnecessary effort being expended on options or processes that are fundamentally incompatible with key privacy principles.

3. Data analysis

Institutions must identify all personal information associated with business processes. This should be accomplished by developing a detailed description and analysis of the data flows. Key components are the business process diagrams, data flow tables and system and infrastructure architectures.

Business process diagrams are high level descriptions of the information flows associated with a given activity. Data flow tables illustrate how and by whom personal information will be collected, used, disclosed and retained. System and infrastructure architectures typically document any physical or logical separation of personal information or security mechanisms that prevent improper access to personal information or maintain any required separation. Together, these elements provide a context for the descriptive analysis.

4. Privacy analysis

Departments and agencies must ensure and document that privacy principles, legislation and policies are adhered to and that privacy impacts and risks associated with program and service delivery activities have been resolved or mitigated.

The *Privacy Impact Assessment Guidelines* include questionnaires that encompass fundamental privacy principles. They reflect the requirements of the *Privacy Act* as well as the principles attached to the *Personal Information Protection and Electronic Documents Act*. The questionnaires are designed to guide institutions in conducting assessments encompassing federal intra-departmental and inter-departmental initiatives and, if necessary, to supplement their assessments with questions appropriate to proposals involving other governments and the private sector.

5. Privacy impact analysis report

Institutions must document their evaluation of the privacy risks, the implications of those risks and their discussions of possible remedies, options and recommendations to avoid or mitigate such risks. The report assesses the level of risk. It constitutes a policy-level discussion of the program or service that facilitates informed policy and system design decisions.

While the format of the report will be determined by the institution's needs, it must at a minimum convey the following information:

- an outline of the proposal involving the collection, use or disclosure of personal information and its objectives, including the legal authority and the justification for the proposal;
- a list of stakeholders and their roles and responsibilities;
- a list of relevant legislation and policies that have implications for privacy and the protection of personal information;
- a description of specific privacy risks that have been identified;
- an analysis of options considered to avoid or mitigate privacy risks;
- a list of residual risks that cannot be resolved by means of the proposed options and an analysis of possible implications of these risks in terms of public reaction and program success; and
- a communications strategy, where appropriate, to deal with public concerns and perceptions about privacy.

The resulting report will constitute the basis for the notification process.

6. Treasury Board and Treasury Board Secretariat

The results of Privacy Impact Assessments must either provide assurance that there are no outstanding privacy implications associated with program and service delivery activities or conversely, serve as early warning indicators that there are significant privacy risks that require resolution. In the case of the latter, changes to the program design or implementation will be needed to address these risks.

Institutions must develop Privacy Impact Assessments in the context of the government-wide policies, guidelines, handbooks and checklists pertaining to sound project management. The aims of the *Privacy Impact Assessment Policy* are consistent with those of the *Enhanced Management Framework Policy* to enhance the Government of Canada's project management capability, to support successful project management and to meet project objectives, including those related to privacy.

Institutions seeking Preliminary Project Approval from the Treasury Board pursuant to the *Project Approval Policy* must include the results of the Privacy Impact Assessment in the body of the submission or the project brief, whereapplicable. Institutions seeking Effective Project Approval from the Treasury Board must provide a status report in the body of the submission or the project brief summarizing the actions taken or to be taken to avoid or mitigate the privacy risks, if any, as per the Privacy Impact Assessment.

7. Notification

The *Privacy Act* requires government institutions to notify individuals of the intended uses, consistent uses and disclosures of personal information when it is being collected. The Act also requires institutions to account publicly for the collection, use and disclosure of personal information by ensuring that their descriptions of Personal Information Banks in *Info Source* are accurate and up-to-date.

Government institutions must provide a copy of the final Privacy Impact Assessment to the Privacy Commissioner. This notification must occur at a reasonably early stage prior to implementing the initiative, program or service. Advance notification is intended to permit the Commissioner to review the issues and, if appropriate, to provide advice to the head of the institution.

To complement this requirement and to promote a broader understanding of how privacy issues related to the program or service have been addressed, institutions must make summaries of the results of their Privacy Impact Assessments available to the public in a timely manner, using plain language and in each of the two official languages in accordance with the *Official*

Languages Act. Institutions must routinely release summaries of their assessments, taking into account that there may be components that must be protected under the *Access to Information Act* or the *Privacy Act*, or that in certain cases, assessments could contain information that would render systems or security measures vulnerable, or refer to programs or services that have not been formally approved or announced. The Internet and conventional publishing should be used to disseminate assessments and may include references and links to related documentation.

Accountability

1. Heads of institutions

Ministers for departments and other heads of institutions as designated by Order in Council for purposes of the Act are responsible for ensuring that their institutions comply with the *Privacy Act, Regulations* and associated policies.

2. Deputy heads of institutions

Deputy Ministers and other deputy heads of institutions are responsible for promoting an awareness of the requirements of this policy within their institutions, for determining whether initiatives have a potential impact on the privacy of Canadians and warrant the development of Privacy Impact Assessments and for integrating and balancing privacy with other legislative and policy requirements. They are responsible for ensuring that the process and tools used in assessing privacy impacts are as rigorous as those outlined in the *Privacy Impact Assessment Guidelines*. In addition, deputy heads are responsible for establishing processes for:

- consulting with the Office of the Privacy Commissioner;
- approving the final Privacy Impact Assessments to be provided to the Commissioner;
- responding to any advice that might be offered by the Commissioner; and
- ensuring that summaries of the results of assessments are available to the public.

3. Institutional officials

Developing and maintaining Privacy Impact Assessments is a shared management responsibility that requires the co-operation and support of various officials throughout institutions. Program and project managers, privacy policy and legal advisors and functional specialists must be involved to ensure that privacy implications are identified, assessed, avoided or resolved. Collaboration with communications staff is required to facilitate the timely dissemination of information to the public.

Institutional officials are also responsible for determining the need and for conducting Preliminary Privacy Impact Assessments if they would facilitate providing advice to deputy heads or consulting with the representatives from the Office of the Privacy Commissioner.

4. Privacy Commissioner of Canada

The Privacy Commissioner of Canada has the authority under the *Privacy Act* to examine the collection, use, disclosure and retention and disposal of personal information by government institutions subject to the Act.

To ensure a comprehensive and current understanding of the privacy implications inherent in proposed or redesigned programs and services, representatives of the Office of the Privacy Commissioner should be involved at the earliest reasonable stages of the development of Preliminary Privacy Impact Assessments or Privacy Impact Assessments. By reviewing the documentation in co-operation with institutional officials, they may provide advice and guidance to institutions and identify solutions to potential privacy risks.

Upon receipt of final Privacy Impact Assessments, the Privacy Commissioner may, at the Commissioner's discretion, provide advice to the head or deputy head of the institution.

5. Treasury Board Secretariat

The Treasury Board Secretariat is responsible for interpreting the policy and for providing advice to institutions, the President of the Treasury Board and the Treasury Board. The Secretariat develops and maintains guidelines to assist institutions in implementing the policy. It is also responsible for monitoring compliance.

The Treasury Board Secretariat will undertake a comprehensive review of the provisions and operation of the *Privacy Impact Assessment Policy* within five years of its coming into effect.

Monitoring

Institutions will assess their degree of compliance with this policy by means of internal audits, reviews and evaluations.

The Treasury Board Secretariat will monitor compliance through a variety of means. For example, the Annual Reports to Parliament required by section 72 of the *Privacy Act*, copies of which are forwarded by institutions to the Treasury Board Secretariat, may be used to monitor compliance with the policy. Observations resulting from this monitoring process may be used in the course of providing advice to the President and Treasury Board Ministers.

The Privacy Commissioner will monitor compliance through the notification process. The Commissioner is empowered by section 37 of the *Privacy Act* to initiate, at any time, an investigation to determine if government institutions are complying with sections 4 through 8 of the Act. In addition, the Commissioner may report on institutional activities in Annual or Special Reports to Parliament.

References

1. Authority

This policy is issued pursuant to section 7 of the *Financial Administration Act* and paragraph 71(1)(d) of the *Privacy Act* where the designated Minister, who is the President of the Treasury Board, may issue directives and guidelines concerning the Act and Regulations.

This policy should be read in conjunction with:

2. Legislation

Access to Information Act
Anti-terrorism Act
Canadian Charter of Rights and Freedoms
National Archives of Canada Act
Official Languages Act
Personal Information Protection and Electronic Documents Act
Privacy Act
Provincial and Territorial Freedom of Information and Protection of Privacy legislation

3. Policies

Access to Information Policy
Active Monitoring Policy
Enhanced Management Framework Policy
Management of Government Information Holdings Policy
Official Languages Policies
Privacy and Data Protection Policy
Project Approval Policy
Security Policy of the Government of Canada

4. Other

Government Records Disposition Program of the National Archives of Canada

Integrated Risk Management Framework

Model Code for the Protection of Personal Information, Canadian Standards Association, 1996

Enquiries

Enquiries concerning the intent and implementation of this policy should be directed to Information Policy Division, Chief Information Officer Branch, Treasury Board Secretariat.

Annex - Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks

Date Modified: 2002-05-02