



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Canada

Directive on Privacy Practices

Published: Apr 01, 2010

© Her Majesty the Queen in Right of Canada,
represented by the President of the Treasury Board, 2010

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-10/2010E-PDF
ISBN: 978-0-660-09674-2

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Directive sur les pratiques relatives à la protection de la vie privée

Directive on Privacy Practices

1. Effective Date

1.1 This directive takes effect on May 6, 2014.

1.2 It replaces the *Directive on Privacy Practices* dated January 31, 2013.

2. Application

2.1 This directive applies to government institutions as defined in [section 3 of the Privacy Act](#), including parent Crown corporations and their wholly owned subsidiaries, if any.

2.2 This directive does not apply to the Bank of Canada.

3. Context

3.1 The [Privacy Act](#) (Act) and the [Privacy Regulations](#) (Regulations) provide the legal framework for the creation, collection, retention, use, disclosure, accuracy and disposition of personal information in the administration of programs and activities by government institutions.

3.2 Under the Act, heads of all government institutions are required to identify, describe and publicly report their institutions' personal information banks (PIBs) and classes of personal information in the Treasury Board of Canada Secretariat's (TBS) annual publication entitled *Info Source*. The descriptions of PIBs and classes of personal information contained in *Info Source* describe how government institutions inform the public and their employees about the personal information they collect and how that information is handled, used, retained and disposed of. *Info Source* assists individuals in exercising their rights under the Act.

3.3 Under the [Policy on Privacy Protection](#), heads of government institutions are to establish practices for the protection and management of personal information under their respective institution's control to ensure that the Act is administered in a consistent and fair manner. This directive supports the policy by setting out the requirements for sound privacy practices and management of personal information.

3.4 The President of the Treasury Board (President), as designated Minister for the purposes of [paragraphs 71\(1\)\(a\) and \(b\) of the Act](#), holds general responsibility for registering all PIBs and for reviewing the manner in which they are maintained and managed in all government institutions. In addition to this general oversight role, the President is responsible for reviewing and approving new or substantially modified PIBs for the government institutions that are departments, as defined in [section 2 of the Financial Administration Act \(FAA\)](#), or may exercise his or her discretion to delegate this authority, subject to terms and conditions, under subsection 71(6) of the Act. In exercising this discretion, the President will consider an institution's compliance with the *Policy on Privacy Protection*, with this and other directives, as well as with any prescribed forms. Even if the President delegates his or her authority, the President remains responsible for the ongoing review of PIBs for all government institutions that are subject to the Act.

3.5 This directive is issued pursuant to paragraph 71(1)(d) of the Act.

3.6 This directive is to be read in conjunction with the Act, the Regulations, other applicable legislation, including the institution's enabling legislation, the *Policy on Privacy Protection*, the [Directive on Privacy Impact Assessment](#), the [Directive on Social Insurance Number](#), the [Directive on Privacy Requests and Correction of Personal Information](#) and the [Standard on Privacy and Web Analytics](#).

4. Definitions

4.1 The definitions to be used in the interpretation of this directive are listed in [Appendix A](#). Additional definitions are listed in [Appendix A of the Policy on Privacy Protection](#).

5. Directive Statement

5.1 Objective

5.1.1 To facilitate the implementation and public reporting of consistent and sound privacy management practices for the creation, collection, retention, use, disclosure, accuracy and disposition of personal information under the control of government institutions.

5.2 Expected Results

5.2.1 Personal information is only created, collected, retained, used, disclosed and disposed of in a manner that respects the provisions of the Act and the Regulations.

5.2.2 PIBs and classes of personal information of government institutions are described in a manner that facilitates the process for individuals to request access to and correction of personal information.

5.2.3 The purposes for which government institutions collect personal information and the privacy practices that support the administration of programs and activities are described in the PIBs and classes of personal information.

6. Requirements

6.1 Heads of government institutions or their delegates are responsible for the following:

6.1.1 Establishing effective privacy practices in their institution, as set out below. These practices are to be followed when officers or employees are involved in activities related to the creation, collection, retention, accuracy, use, disclosure or disposition of personal information under the control of the government institution, including the personal information of officers or employees of the institution.

Privacy breaches

6.1.2 Establishing plans and procedures for addressing privacy breaches in their institution, which include the following:

- Roles and responsibilities in the event of a privacy breach;
- Internal procedures and communications, including timing, for notifying the Office of the Privacy Commissioner of Canada (OPC), TBS and parties affected by the privacy breaches; and
- Notification requirements which must include a process for the mandatory reporting of material privacy breaches to the OPC and to TBS. These procedures must also align with the [Policy on Government Security](#) and its related directives and standards.

Personal information banks and classes of personal information

6.1.3 Ensuring that the development process for new or substantially modified PIBs is aligned with the process for the development and approval of the core privacy impact assessment, as required by the *Directive on Privacy Impact Assessment*.

6.1.4 Submitting a request to TBS for the registration of each new PIB, or the termination of an existing PIB, and ensuring that requests are accompanied by the following information:

- In the case of a request to register a new PIB, all elements of the PIB as described in [subparagraphs 11\(1\)\(a\)\(i\) through \(vi\) of the Act](#), accompanied by a completed and approved core privacy impact assessment;
- In the case of a request to terminate an existing PIB, an explanation of why the PIB should be terminated and a confirmation that the records and personal information contained therein have been disposed of in accordance with the institution's Retention Disposition Authority and are no longer under the institution's control.

6.1.5 Satisfying, for the institutions that are departments as defined in section 2 of the FAA, the additional requirements, as set out in [Appendix B](#), for approvals by the President in relation to PIBs, unless this approval authority has been delegated to the head of the institution by the President, subject to terms and conditions.

6.1.6 Notifying TBS of changes to PIBs and, where these changes are substantial, ensuring that TBS receives a core privacy impact assessment as required by the *Directive on Privacy Impact Assessment*.

Exempt banks

6.1.7 Ensuring that proposals submitted to TBS to establish or revoke an exempt bank include the following:

- A description of the information to be included in the exempt bank and why that information should be included in an exempt bank;
- Confirmation that the files in the bank consist predominantly of personal information as described in [sections 21 or 22 of the Act](#);
- The specific exemption provision in the Act being relied on and, for any injury test exemption, a statement of the expected detrimental effect; and
- A draft Order in Council, along with a draft Regulatory Impact Analysis Statement.

Requests and disclosures to investigative bodies

6.1.8 Adhering to the requirements concerning requests from and disclosures to investigative bodies outlined in [Appendix C](#).

Recording new uses and disclosures

6.1.9 Establishing procedures for maintaining a record of new uses and disclosures, as well as any consistent uses that are not reflected in a PIB. Such procedures will ensure that:

- Descriptions of use, purpose of collection and disclosure recorded in all PIBs are kept up-to-date (this does not apply to disclosures to investigative bodies);
- Any new consistent uses are reflected in the relevant PIBs; and

- The Privacy Commissioner of Canada is notified of all new consistent uses.

Web analytics and privacy

6.1.10 Ensuring that the use of Web analytics for measuring and improving performance of Government of Canada websites complies with the *Standard on Privacy and Web Analytics*.

6.2 Executives and senior officials who manage programs or activities involving the creation, collection or handling of personal information are responsible for:

Privacy practices

6.2.1 Informing the individual who is responsible for the institution's PIBs of any new program or activity or of any substantial modification to an existing program or activity where personal information is collected or handled in a decision-making process that directly affects the individual.

6.2.2 Informing the individuals who are responsible for managing the institution's websites, as well as functional specialists and Web content owners, of the need to comply with the requirements of the *Standard on Privacy and Web Analytics*.

6.2.3 Ensuring that privacy practices are consistent with and respect the provisions found in the Act, the Regulations and other applicable legislation, including the institution's enabling legislation.

6.2.4 Informing employees of the legal and administrative consequences of any inappropriate or unauthorized access to, or use, disclosure, modification, retention and disposition of, personal information related to a particular program or activity.

Privacy breaches

6.2.5 Implementing the institution's plan for addressing privacy breaches. See [Guidelines for Privacy Breaches](#) issued by TBS.

Collection and creation of personal information

6.2.6 Ensuring, before collecting personal information, that the institution has parliamentary authority for the program or activity for which the information is being collected. Obtaining an individual's consent to a collection of personal information does not replace or establish authority for the collection of that information.

6.2.7 Identifying the elements to be included in a PIB before there is any new collection of personal information.

6.2.8 Limiting the collection of personal information to what is directly related to and demonstrably necessary for the government institution's programs or activities. Personal information that is created by the government institution is also considered a collection under the Act.

Privacy notice

6.2.9 Notifying the individual whose personal information is collected directly of the following:

- The purpose and authority for the collection;
- Any uses or disclosures that are consistent with the original purpose;
- Any legal or administrative consequences for refusing to provide the personal information;
- The rights of access to, correction and protection of personal information under the Act; and
- The right to file a complaint to the Privacy Commissioner of Canada regarding the institution's handling of the individual's personal information.

6.2.10 Adapting the privacy notice for either written or verbal communication at the time of collection. Notices are to include a reference to the PIB described in *Info Source*.

Consent regarding collection, use and disclosure

6.2.11 Consent is not required if the personal information is to be used for the authorized purpose for which it was obtained, for a use consistent with that purpose or for a purpose for which it may be disclosed to the institution under [subsection 8\(2\) of the Act](#).

6.2.12 Obtaining consent from an individual for the following:

- The indirect collection of personal information, unless seeking consent would result in collecting inaccurate information, would defeat the purpose of collection or would prejudice the use of the information collected;
- Uses or disclosures that are not consistent with the purposes for which the information was originally obtained or compiled; and
- Any disposition of personal information before the two-year minimum retention standard established by the Regulations unless such disposition is expressly authorized by legislation.

6.2.13 Including the following elements, as applicable, when seeking consent:

- The purpose of the consent and the specific personal information involved;

- The sources who will be asked to provide the information, in the case of indirect collections, as well as the reason for making the collection indirectly;
- Uses or disclosures that are not consistent with the original purpose of the collection and for which consent is being sought;
- Any consequences that may result from withholding consent; and
- Any alternatives to providing consent.

6.2.14 Ensuring that consent is obtained in writing or is otherwise adequately documented, including such information as the date and time of consent. A record is required to support verbal consent.

Accuracy

6.2.15 Ensuring, through all reasonable measures, that personal information to be used in a decision-making process, is as accurate, up to date and complete as possible. Those measures will involve one or more of the following:

- Direct collection or validation from the individual;
- Indirect collection or validation when authorized or when consent was obtained, which may involve verifying the personal information against a reliable source (either public or private); and
- Technological means to identify errors and discrepancies.

6.2.16 Implementing, in cases when direct collection or obtaining consent is not feasible, measures to:

- Ensure that the personal information is obtained from a reliable source; or
- Verify or validate the accuracy of the personal information before use.

6.2.17 Documenting the source or technique used to validate the personal information and identifying, where appropriate, the source, as well as any data matching in the relevant PIB description.

6.2.18 Ensuring that individuals are given the opportunity, whenever possible, to correct inaccurate personal information before any decision is made that could have an impact on them.

Safeguards for use and disclosure

6.2.19 Identifying which positions or functions in the program or activity have a valid reason to access and handle personal information and limiting access to individuals occupying those positions.

6.2.20 Limiting access to, and use of, personal information by administrative, technical and physical means, to protect that information.

6.2.21 Adopting appropriate measures to ensure that access to, as well as use and disclosure of, personal information are monitored and documented in order to address the timely identification of inappropriate or unauthorized access to, or handling of, personal information.

6.2.22 Following the requirements set out below when personal information is disclosed to another institution, to a public or private sector entity, or to an individual:

- The privacy notice reflects, as appropriate, the disclosure;
- An agreement or arrangement with appropriate safeguards has been established between the government institution and the public sector entity, whether that entity is international, federal, provincial or territorial, or municipal, before the information is shared; and
- Contracts that are established with private sector entities or with individuals outline measures and provisions to address the following:
 - Control over the personal information;
 - Limitations on collection, use, subsequent disclosure and retention of personal information for the purposes of the contract;
 - Prohibitions regarding the personal information;
 - Disposition of the personal information, where relevant;
 - Administrative, technical and physical safeguards; and
 - Obligations of other parties acting on behalf of the government institution.
- Government institutions subject to the *Policy on Government Security* are also to ensure that government security standards are respected and that all guidance issued by lead security agencies as set out in [Appendix B of that policy](#) is followed.

6.2.23 Ensuring, when personal information is transferred out of the control of a government institution as a result of the devolution or privatization of a program or activity, that:

- Authority is established for the transfer;
- Adequate privacy practices are in place prior to transfer;
- The rights of employees to access and correct their personal information will be maintained after the transfer;
- A records transfer agreement, which respects any existing records disposition authority, is in place to establish the terms and conditions for the records being transferred, including security considerations; and
- Consent is obtained from the Librarian and Archivist of Canada before the transfer of records.

Recording of new uses and disclosures

6.2.24 Notifying the head or appropriate delegate of any use, purpose or disclosure of personal information that is not reflected in the PIB description and updating the PIB accordingly.

Retention and disposition of personal information

6.2.25 Applying the institution's standards for the retention of personal information, as well as the disposition standards as established by Library and Archives Canada, and reporting them in the relevant PIB.

6.2.26 Ensuring that personal information of an individual that has been used for an administrative purpose is retained by the institution in accordance with [subsections 6\(1\) of the Act](#) and [paragraphs 4\(1\)\(a\) and \(b\) of the Regulations](#).

6.2.27 Reviewing files described within PIBs, including those of exempt banks, on a regular basis and disposing of records containing personal information in accordance with direction from Library and Archives Canada, as stipulated in [sections 12 through 14 of the Library and Archives of Canada Act](#).

6.2.28 Institutions that are subject to the *Policy on Government Security* are to dispose of records in accordance with government security standards.

6.3 Monitoring and reporting requirements

6.3.1 The monitoring and reporting requirements of the *Policy on Privacy Protection* apply to this directive.

7. Consequences

7.1 The consequences identified in the *Policy on Privacy Protection* apply to this directive.

8. Roles and responsibilities of government organizations

8.1 Further to the roles described in [section 8 of the Policy on Privacy Protection](#) and [subsection 3.4 of this Directive](#), the President, with the support of TBS, is responsible for:

- Setting the terms and conditions for the approval of PIBs, as well as the terms and conditions for delegating this approval to heads of departments;
- Revoking any delegation order made under subsection 71(6) of the Act if there is a systemic compliance issue at a government institution.

8.2 The roles and responsibilities of other government organizations are described in section 8 of the *Policy on Privacy Protection*.

9. References

9.1 Relevant legislation and regulations

- [Access to Information Act](#)
- [Access to Information Regulations](#)
- [Canadian Charter of Rights and Freedoms](#)
- [Financial Administration Act](#)
- [Library and Archives of Canada Act](#)
- [Official Languages Act](#)
- [Privacy Act](#)
- [Privacy Regulations](#)

9.2 Related TBS policies and publications

- [Communications Policy of the Government of Canada](#)
- [Directive on Privacy Impact Assessment](#)
- [Directive on Privacy Requests and Correction of Personal Information](#)
- [Directive on Social Insurance Number](#)
- [Guidelines for Privacy Breaches](#)
- [Policy Framework for Information and Technology](#)
- [Policy on Access to Information](#)
- [Policy on Government Security](#)
- [Policy on Information Management](#)
- [Policy on Learning, Training and Development](#)
- [Policy on Management of Information Technology](#)
- [Policy on Privacy Protection](#)
- [Privacy Breach Management Toolkit](#)
- [Standard on Privacy and Web Analytics](#)

10. Enquiries

10.1 Please direct enquiries about this directive to your institution's access to information and privacy (ATIP) coordinator. For interpretation of this directive, the ATIP coordinator is to contact:

Information and Privacy Policy Division
Chief Information Officer Branch
Treasury Board Secretariat
219 Laurier Avenue West
Ottawa, Ontario K1A 0R5
E-mail: ippd-dpiprp@tbs-sct.gc.ca
Telephone: 613-946-4945
Fax: 613-957-8020

Appendix A: Definitions

administrative safeguards

Policies, directives, rules, procedures and processes that aim to protect personal information throughout the life cycle of both the information and the program or activity (e.g., institutional security policy, security provisions in a service contract for the destruction of records).

classes of personal information

Personal information that is not intended to be used for an administrative purpose or that cannot be retrieved by the name of the individual or another personal identifier (e.g., unsolicited opinions and general correspondence).

creation of personal information

Any personal information element or sub-element that a government institution assigns to an identifiable individual regardless of whether the information is derived from existing personal information under the control of the government institution or the institution appends new information to the individual.

direct collection

The collection of personal information from the individual to whom the information relates.

disclosure

The release of personal information by any method (e.g., transmission, provision of a copy, examination of a record) to any body or person.

handling

Any process involving personal information, including collection, correction, creation, modification, use, retention, disclosure and disposition.

indirect collection

The collection of personal information from a source other than the individual to whom the information relates.

material privacy breach

A privacy breach that involves sensitive personal information and could reasonably be expected to cause injury or harm to the individual.

original purpose

The purpose that was first identified when initiating the collection of personal information and that is directly related to an operating program or activity of the institution. A purpose that is not consistent with the original purpose is considered to be a secondary purpose.

physical safeguards

The facilities and equipment that are used to protect personal information (e.g., locked storage rooms, locked filing cabinets).

predominantly

In the context of an exempt bank, means that more than half of the information in each file contained in the bank qualifies for an exemption under section 21 or 22 of the Act.

privacy breach

The improper or unauthorized creation, collection, use, disclosure, retention or disposition of personal information.

privacy notice

A verbal or written notice informing an individual of the purpose of a collection of personal information and of the government institution's authority for collecting, including creating, using and disclosing the information. The notice, which must reference the PIB described in *Info Source*, also informs the individual of his or her right to access, and request the correction of, the personal information and of the consequences of refusing to provide the information requested.

privacy practices

All practices related to the creation, collection, retention, accuracy, correction, use, disclosure, retention and disposition of personal information.

Regulatory Impact Analysis Statement (RIAS)

A tool used for regulatory reform that assesses the impact of a proposed regulation on the quality of the environment and on the health, safety, security, and social and economic well-being of Canadians.

reliable source

A source of information or a data holding that is deemed to be accurate and up-to-date and that can be trusted and relied on for the purposes of collecting or validating personal information.

technical safeguards

Information technology measures that are used to protect the facility, the equipment, and the support system where personal information is recorded and stored (e.g., electronic access control devices, audit controls).

Web analytics

The collection, analysis, measurement and reporting of data about Web traffic and user visits for the purposes of understanding and optimizing Web usage.

Appendix B: Additional Requirements Under the Act for Departments As Defined in Section 2 of the FAA

In addition to requiring the registration and publication of personal information banks (PIBs) in *Info Source*, [subsections 71\(3\) and \(4\) of the Act](#) require that the President approve each new PIB or each substantial modification to or termination of an existing PIB submitted by the government institutions defined as departments under section 2 of the FAA.

Unless the President has delegated this approval to the head of the department, pursuant to subsection 71(6) of the Act, the head or delegate responsible under [section 10 of the Act](#) is responsible for the following:

- Presenting all proposals for the creation of a new PIB or for the modification or termination of an existing PIB to TBS for approval; and,
- Providing justification or analysis in support of the proposal. In the case of a proposal to establish or substantially modify a PIB that involves administrative decisions, a completed core privacy impact assessment will be required (see the *Directive on Privacy Impact Assessment*).

Appendix C: Requirements Related to Paragraph 8(2)(e) of the Act

Under paragraph 8(2)(e) of the Act, personal information may be disclosed to an investigative body specified in the Regulations, upon written request of that body, for the purpose of enforcing any Canadian or provincial law or carrying out a lawful investigation. This provision does not grant investigative bodies a right of access to personal information. It leaves the disclosure decision to the discretion of the institution that has control of the information once the relevant criteria have been satisfied.

Requests under paragraph 8(2)(e)

Requests made under paragraph 8(2)(e) of the Act are to be in writing and are to contain the following:

- The name of the investigative body;
- The name of the individual who is the subject of the request, or some other personal identifier;
- The purpose of the request and a description of the information to be disclosed;
- The section of the federal or provincial statute under which the investigative activity is being undertaken; and
- The name, title and signature of the member of the investigative body who is filing the request.

All copies of such requests received by an institution are to be retained.

Documenting 8(2)(e) disclosures

When such requests are received, the head of the institution or the delegate responsible for decisions with respect to paragraph 8(2)(e) of the Act is to retain a record of disclosure for the personal information provided to the investigative body. The record of disclosure is to contain the following:

- Clear indication as to whether the request was granted or refused;
- The date the request was received;
- The personal information banks (PIBs) in which the disclosed information is held;
- The specific personal information, record or file that was disclosed;
- The name, title and signature of the official who authorized the response; and
- The name of the institution.

A separate PIB is maintained for all records of disclosure to federal investigative bodies, including copies of the information that was disclosed to the requester. Pursuant to [subsection 8\(4\) of the Act](#) and [section 7 of the Regulations](#), information contained in this PIB must be retained for a minimum of two years and must be made available to the Privacy Commissioner on request.