



[Canada.ca](#) › [How government works](#) › [Policies, directives, standards and guidelines](#)

› [Directive on Privacy Practices](#)

Directive on Privacy Practices

1. Effective date

- 1.1 This directive takes effect on October 9, 2024.
- 1.2 This directive replaces the following:
 - 1.2.1 The *Directive on Privacy Practices* dated October 22, 2022; and
 - 1.2.2 The *Directive on Privacy Impact Assessment* dated April 1, 2010.

2. Authorities

- 2.1 This directive is issued pursuant to paragraph 71(1)(d) of the *Privacy Act* (the Act) and as specified in subsection 2.2 of the *Policy on Privacy Protection*.

3. Objectives and expected results

- 3.1 In addition to the objectives indicated in subsection 3.1 of the *Policy on Privacy Protection*, the objectives of this directive are to facilitate the implementation and public reporting of consistent and sound

privacy management practices for the protection of personal information throughout its life cycle, which includes the creation, collection, retention, use, disclosure and disposal of personal information under the control of government institutions, whether the information is held by the institution or by a third party acting under contract, information-sharing agreement or information-sharing arrangement with the institution.

3.2 The expected results of this directive are as follows:

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

3.2.2 Personal information banks (PIBs) and classes of personal information of government institutions are described in a manner that:

3.2.2.1 Facilitates the process for individuals to request access to and correction of personal information; and

3.2.2.2 Explains the purposes for which government institutions collect personal information and the privacy practices that support the administration of programs and activities.

3.2.3 Privacy impact assessments (PIAs) are completed so that the privacy risks associated with programs and activities that use personal information for administrative purposes are

identified, reviewed and updated, and appropriate mitigation measures implemented.

- 3.2.4 Privacy protocols are completed, reviewed and updated for the collection, use or disclosure of personal information for a non-administrative purpose.
- 3.2.5 Privacy breaches are effectively managed, and appropriate preventative measures are in place.
- 3.2.6 Personal information under the control of government institutions is accurate.

4. Requirements

- 4.1 Heads of government institutions or their delegates are responsible for the following:
 - 4.1.1 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 disposal of personal information under the control of the government institution, including the personal information of officers or employees of the institution as defined by the Act;

Privacy training

- 4.1.2 Ensuring that employees of government institutions receive privacy training as outlined in Appendix B of the Directive on

Personal Information Requests and Correction of Personal Information;

- 4.1.3 Documenting the completion of training in accordance with Appendix B of the *Directive on Personal Information Requests and Correction of Personal Information*;

Privacy breaches

- 4.1.4 Ensuring that plans for addressing privacy breaches that affect personal information under the control of the institution, including those that occur within or as a result of third-party entities, meet the following requirements:
- 4.1.4.1 Roles and responsibilities in the event of a privacy breach are clearly defined;
 - 4.1.4.2 Internal procedures and communications align with the *Policy on Government Security* and its related directives and standards; and
 - 4.1.4.3 The requirements set out in Appendix B: Mandatory Procedures for Privacy Breaches are met;
- 4.1.5 In the event of a privacy breach affecting personal information that is held by the institution but is under the control of another government institution, promptly notifying the institution under whose control the personal information lies and undertaking responsive action in coordination with the institution as required to ensure that

the requirements set out in Appendix B: Mandatory Procedures for Privacy Breaches are met;

- 4.1.6 Executing the mandatory procedures required of heads of government institutions or their delegates set out in Appendix B: Mandatory Procedures for Privacy Breaches;

Personal information banks and classes of personal information

- 4.1.7 Ensuring that the development process for new or substantially modified PIBs is aligned with the process for the development and approval of PIAs and privacy protocols;
- 4.1.8 Ensuring that a PIB is established for:
- 4.1.8.1 Any program or activity that uses personal information for an administrative purpose; or
 - 4.1.8.2 Any program or activity that uses personal information that is organized and retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual;
- 4.1.9 Ensuring that a class of personal information is established for any personal information that is under the control of a government institution but that is not intended to be used for an administrative purpose and that cannot be retrieved by the name of the individual or another personal identifier; and

- 4.1.10 Updating the Treasury Board of Canada Secretariat (TBS)-prescribed repository of PIBs for all new, modified or terminated PIBs, and for all changes to classes of personal information;

Privacy impact assessments

- 4.1.11 Ensuring the establishment of a PIA development and approval process, that:
 - 4.1.11.1 Takes into consideration the responsibility within the institution for establishing PIBs; and
 - 4.1.11.2 Is commensurate with the level of risk related to the privacy invasiveness of the institution's program or activities; and
- 4.1.12 Ensuring that a PIA is established for any program or activity that uses personal information for an administrative purpose;

Privacy protocols

- 4.1.13 Ensuring that a privacy protocol is established for any program or activity that uses personal information for a non-administrative purpose;

Exempt banks

- 4.1.14 Ensuring that proposals submitted to TBS to establish or revoke an exempt bank include:

- 4.1.14.1 A description of the information to be included in the exempt bank and why that information should be included in an exempt bank;
- 4.1.14.2 Confirmation that the files in the bank consist predominantly of personal information as described in sections 21 or 22 of the Act;
- 4.1.14.3 The specific exemption provision in the Act being relied on;
- 4.1.14.4 A statement of the expected detrimental effect for any injury text exemption; and
- 4.1.14.5 A draft order-in-council, along with a draft Regulatory Impact Analysis Statement;

Requests and disclosures to investigative bodies

- 4.1.15 Adhering to the requirements concerning requests from and disclosures to investigative bodies outlined in Appendix D: Requirements Related to Paragraph 8(2)(e) of the *Privacy Act*;

Recording new uses and disclosures

- 4.1.16 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:
 - 4.1.16.1 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);

4.1.16.2 Any new consistent uses are reflected in the relevant PIBs; and

4.1.16.3 The Privacy Commissioner of Canada is notified of all new consistent uses;

Privacy in web analytics

4.1.17 Ensuring that the use of web analytics for measuring and improving performance of Government of Canada websites complies with Appendix E: Standard on Privacy in Web Analytics; and

Monitoring and reporting

4.1.18 Monitoring and reporting on the requirements of this directive are conducted as specified in the *Policy on Privacy Protection*.

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

Privacy practices

4.2.1 Informing the head of the government institution or their delegate of any new or proposed 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;

- 4.2.2 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; and
- 4.2.3 Informing employees of the legal and administrative consequences of any inappropriate or unauthorized access to, use, disclosure, modification, retention and disposal of personal information related to a particular program or activity;

Privacy breaches

- 4.2.4 Implementing the institution's plans for addressing privacy breaches;
- 4.2.5 Ensuring that the head of the government institution or their delegate is notified of any potential or confirmed privacy breach that affects personal information held by or under the control of the institution, including any that occur within a third party; and
- 4.2.6 Executing the mandatory procedures required of executives and senior officials who manage programs or activities that involve the creation, collection or handling of personal information set out in Appendix B: Mandatory Procedures for Privacy Breaches;

Collection and creation of personal information

- 4.2.7 Ensuring, before collecting personal information, that the institution has legal authority for the program or activity for which the information is being collected. Obtaining an individual's consent for collecting personal information does not replace nor establish legal authority for collecting that information;
- 4.2.8 Identifying the elements to be included in a PIB before there is any new collection of personal information; and
- 4.2.9 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;

Personal information banks

- 4.2.10 Ensuring that PIBs are prepared, updated, terminated and submitted to TBS in accordance with Appendix C: Standard on Privacy Impact Assessment;

Privacy impact assessments

- 4.2.11 When personal information is to be used for an administrative purpose, ensuring that PIAs are prepared and updated:
 - 4.2.11.1 In accordance with Appendix C: Standard on Privacy Impact Assessment; and

- 4.2.11.2 In collaboration with the official responsible for section 10 of the *Privacy Act*;
- 4.2.12 Approving PIAs in conjunction with the official responsible for section 10 of the *Privacy Act*; and
 - 4.2.12.1 Providing approved PIAs to TBS and the Office of the Privacy Commissioner (OPC), while respecting Cabinet confidences;
- 4.2.13 Prior to preparing or updating any PIA for a program or activity that involves more than one institution:
 - 4.2.13.1 Determining the approach for the completion of the PIA(s) with other institutions involved; and
 - 4.2.13.2 Ensuring that TBS and the OPC are notified in accordance with Appendix C: Standard on Privacy Impact Assessment;
- 4.2.14 Ensuring that decisions to prepare or update PIAs are documented in accordance with Appendix C: Standard on Privacy Impact Assessment; and
- 4.2.15 Ensuring that summaries of approved PIAs are published in accordance with Appendix C: Standard on Privacy Impact Assessment;

Privacy protocols

- 4.2.16 When personal information is to be used for a non-administrative purpose, ensuring that privacy protocols are prepared and updated:

- 4.2.16.1 In accordance with Appendix C: Standard on Privacy Impact Assessment; and
- 4.2.16.2 In collaboration with the official responsible for section 10 of the *Privacy Act*; and
- 4.2.17 Approving privacy protocols in conjunction with the official responsible for the section 10 of the *Privacy Act*;
- 4.2.18 Ensuring that decisions to establish or update privacy protocols are documented in accordance with Appendix C: Standard on Privacy Impact Assessment; and
- 4.2.19 When a PIB is being registered, modified or transferred in relation to a program or activity that uses personal information for a non-administrative purpose, ensuring that the associated privacy protocol is provided to TBS and the OPC, while respecting Cabinet confidences;

Privacy notice

- 4.2.20 Notifying the individual whose personal information is collected directly of:
 - 4.2.20.1 The purpose and legal authority for the collection;
 - 4.2.20.2 Any uses or disclosures that are consistent with the original purpose;
 - 4.2.20.3 Any legal or administrative consequences for refusing to provide the personal information;
 - 4.2.20.4 The relevant PIB description;

- 4.2.20.5 The rights of access to, correction and protection of personal information under the Act; and
- 4.2.20.6 The right to file a complaint to the Privacy Commissioner of Canada regarding the institution's handling of the individual's personal information; and
- 4.2.21 Adapting the privacy notice for either written or verbal communication at the time of collection;

Consent regarding collection, use and disclosure

- 4.2.22 Obtaining consent from an individual for the following:
 - 4.2.22.1 The indirect collection of personal information, unless the collection is for a non-administrative purpose or a purpose listed under subsection 8(2) of the Act, or seeking consent could result in collecting inaccurate information or defeat the purpose or prejudice the use for which the information was collected;
 - 4.2.22.2 Uses or disclosures that are not consistent with the purposes for which the information was originally obtained or compiled, unless the use or disclosure is authorized under subsection 8(2) of the Act; and
 - 4.2.22.3 Any disposal of personal information before the two-year minimum retention standard

established by the Regulations unless such disposal is expressly authorized by legislation;

- 4.2.23 Including the following elements, as applicable, when seeking consent:
 - 4.2.23.1 The purpose of the consent;
 - 4.2.23.2 The specific personal information elements involved;
 - 4.2.23.3 In the case of indirect collections, the sources that will be asked to provide the information, as well as the reason for making the collection indirectly;
 - 4.2.23.4 Uses or disclosures that are not consistent with the original purpose of the collection and for which consent is being sought;
 - 4.2.23.5 Any consequences that may result from withholding consent; and
 - 4.2.23.6 Any alternatives to providing consent; and
- 4.2.24 Ensuring that consent is obtained in writing or is otherwise adequately documented, including information such as the date and time of consent;

Accuracy

- 4.2.25 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. This includes

collecting personal information directly from the individual, wherever possible, unless the individual authorizes otherwise or for reasons permitted by subsection 5(1) of the Act;

- 4.2.26 Implementing, in cases where personal information is collected indirectly without consent having been obtained, measures to:
 - 4.2.26.1 Ensure that the personal information is obtained from a reliable source; or
 - 4.2.26.2 Verify or validate the accuracy of the personal information before use;
- 4.2.27 When validating the accuracy of personal information, documenting the source or technique used;
- 4.2.28 When validating the accuracy of personal information, identifying in the relevant PIB description the source or technique used, including any data matching, where appropriate; and
- 4.2.29 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 access, use and disclosure

- 4.2.30 Limiting access to personal information to those individuals who hold positions or functions in the program or activity

that have a valid reason to access the personal information;

- 4.2.31 Limiting access to, as well as use and disclosure of, personal information by administrative, technical and physical means, to protect that information; and
- 4.2.32 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 privacy breaches;

Contracts, agreements and arrangements

- 4.2.33 Establishing a contract, information-sharing agreement or information-sharing arrangement with appropriate safeguards prior to any disclosure of personal information to another federal program or to another public or private sector entity, unless the personal information is exchanged under an international treaty in accordance with international standards;
- 4.2.34 Ensuring that appropriate safeguards for contracts, information-sharing agreements and information-sharing arrangements subject to subsection 4.2.33 of this directive that take effect or are substantively modified after October 26, 2022, include provisions that address the following elements:
 - 4.2.34.1 The specific elements of personal information that will be disclosed;

- 4.2.34.2 The specific purpose or purposes for the disclosure;
- 4.2.34.3 Limitations on collection, use and subsequent disclosure of the personal information;
- 4.2.34.4 Proper retention and disposal of the personal information, where relevant, including a confirmation of destruction where destruction is required;
- 4.2.34.5 Administrative, technical and physical safeguards;
- 4.2.34.6 The government institution's continued control over any personal information disclosed to or collected by the entity as part of the contract, information-sharing agreement or information-sharing arrangement;
- 4.2.34.7 The obligation to coordinate with the government institution such that the institution can meet its obligations under section 12 of the *Privacy Act* regarding an individual's right of access;
- 4.2.34.8 For government institutions subject to the *Policy on Government Security*, the obligation to follow all guidance issued by lead security agencies as set out in section 5 of that policy;
- 4.2.34.9 Mandatory timely reporting to the government institution of any potential or confirmed privacy breach affecting the personal information;

- 4.2.34.10 For entities not subject to the *Privacy Act*, the obligation in the event of a potential or confirmed privacy breach to provide, on request, the government institution leading the investigation with sufficient access to the personal information holdings to undertake an assessment of the potential or confirmed privacy breach; and
- 4.2.34.11 A mandatory review of the contract, information-sharing agreement or information-sharing arrangement, at an interval agreed upon by the parties;
- 4.2.35 Making any contract, information-sharing agreement or information-sharing arrangement subject to subsection 4.2.33 available to the OPC and TBS upon request;
- 4.2.36 Making available to the public, via the annual update to the institution's *Info Source*, summaries of all contracts, information-sharing agreements and information-sharing arrangements that are subject to subsection 4.2.33 and that take effect or are substantively modified after October 26, 2022, except in cases of single, one-time disclosures of personal information; and
- 4.2.37 Respecting security requirements as well as any other confidentiality or legal consideration when making a summary of a contract, information-sharing agreement or information-sharing arrangement available to the public;

Devolution or privatization

- 4.2.38 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:
- 4.2.38.1 Authority is established for the transfer;
 - 4.2.38.2 Adequate privacy practices are in place prior to the transfer;
 - 4.2.38.3 The rights of individuals to access and correct their personal information will be maintained after the transfer;
 - 4.2.38.4 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;
 - 4.2.38.5 Consent is obtained from the Librarian and Archivist of Canada before the transfer of records; and
 - 4.2.38.6 A notice of the devolution or privatization is made available to the public via the annual update to the institution's Info Source

Treasury Board submissions

- 4.2.39 When preparing a Treasury Board submission, ensuring that the submission identifies:

4.2.39.1 Whether the authorities requested are related to a program or activity that involves the creation, collection, use, disclosure, retention or disposal of personal information; and

4.2.39.1.2 In the body of the submission, whether a PIA is required for a program or activity that involves personal information;

4.2.39.2 In the project brief, when seeking approval from the Treasury Board, measures that are being taken or that are to be taken to address privacy issues and risks; and

4.2.40 If a Treasury Board submission indicates that a PIA is required, ensuring that it is identified in the body of the submission and:

4.2.40.1 Whether the PIA has been completed; or

4.2.40.2 What the timelines are for the completion of the PIA if it has not yet been completed;

Recording of new uses and disclosures

4.2.41 Notifying the head or appropriate delegate of any use, purpose or disclosure of personal information that is not reflected in the PIB description and ensuring that the PIB is updated accordingly;

Retention and disposal of personal information

- 4.2.42 Applying the institution's standards for the retention of personal information, as well as the disposition authorizations as established by Library and Archives Canada and reporting them in the relevant PIB;
- 4.2.43 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;
- 4.2.44 Reviewing files described within PIBs, including those of exempt banks, on a regular basis and disposing of records that contain 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*; and
- 4.2.45 Where the institution is subject to the *Policy on Government Security*, disposing of records in accordance with government security standards;

Privacy in web analytics

- 4.2.46 Informing employees and any other 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 Appendix E: Standard on Privacy in Web Analytics.

- 4.3 Employees of government institutions are responsible for the following:

Privacy breaches

- 4.3.1 Executing the mandatory procedures required of employees set out in Appendix B: Mandatory Procedures for Privacy Breaches.

Personal information banks, privacy impact assessments and privacy protocols

- 4.3.2 Preparing and updating PIBs, PIAs and privacy protocols in accordance with Appendix C: Standard on Privacy Impact Assessment;

Privacy in web analytics

- 4.3.3 Performing web analytics, if authorized to do so, in compliance with the requirements of Appendix E: Standard on Privacy in Web Analytics; and

Privacy training

- 4.3.4 Completing privacy training as outlined in Appendix B of the *Directive on Personal Information Requests and Correction of Personal Information*.

5. Roles of other government organizations

- 5.1 This section identifies the roles of other key government organizations in relation to this directive. In and of itself, this section

does not confer any authority.

5.2 TBS is responsible for supporting the President of the Treasury Board in:

5.2.1 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;

5.2.2 Revoking any delegation order made under subsection 71(6) of the Act if there is a systemic compliance issue at a government institution; and

5.2.3 Monitoring and tracking material privacy breaches across the government.

5.3 The Office of the Chief Information Officer, TBS, is responsible for approving de-identification methodologies that a third-party service provider is required to use, as set out in subsection E.2.2.3 of Appendix E: Standard on Privacy in Web Analytics, for the purpose of web analytics on servers hosted externally by the third party.

6. Application

6.1 This directive applies as described in section 6 of the *Policy on Privacy Protection*.

7. References

7.1 Legislation

- *Financial Administration Act*

- *Library and Archives of Canada Act*
- *Privacy Act*
- *Privacy Regulations*
- *Shared Services Canada Act*

7.2 Related policy instruments

- *Directive on Service and Digital*
- *Policy on Government Security*
- *Policy on Privacy Protection*

7.3 Related guidance instruments and forms

- *Access to Information and Privacy Implementation Notices*
- *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions*
- *Guidance on Preparing Information Sharing Agreements Involving Personal Information*
- *Guideline on Service and Digital*
- *Info Source Online Publishing Requirements*
- *Privacy Breach Management Toolkit*
- *The Digital Privacy Playbook*
- *Treasury Board of Canada Secretariat Forms*

8. Enquiries

8.1 Members of the public may contact questions@tbs-sct.gc.ca regarding any questions about this directive.

8.2 Employees of federal institutions may contact their Access to Information and Privacy Coordinator regarding any questions about this directive.

- 8.3 Access to Information and Privacy Coordinators may contact ippd-dpiprp@tbs-sct.gc.ca regarding any questions about this directive.
-

Appendix A: Definitions

- A.1 The definitions listed below, in addition to those listed in Appendix A of the *Policy on Privacy Protection*, are to be used in the interpretation of this directive.

administrative safeguards (*mesures de protection administrative*)

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 (for example, institutional security policy, security provisions in a service contract for the destruction of records).

classes of personal information (*catégories de renseignements personnels*)

Descriptions of personal information that is under the control of a government institution but 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 (for example, unsolicited opinions and general correspondence). Classes of personal information must be listed and described in an institution's *Info Source* entry.

creation of personal information (*création de renseignements personnels*)

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. The

creation of personal information is considered a collection under the *Privacy Act*.

de-identification (*dépersonnalisation*)

A process that involves modifying personal information to remove or alter identifiers to reduce identifiability and implementing mitigation controls to a degree that is reasonable in the context. De-identified information carries a residual risk of re-identification.

de-identified information (*renseignements dépersonnalisés*)

Information resulting from the application of de-identification.

digital markers (*marqueurs numériques*)

Mechanisms used to remember a visitor's online interactions with a website(s). These mechanisms may be used to record a visitor's online interactions within a single session or visit or to record a visitor's online interactions through multiple sessions or visits.

direct collection (*collecte directe*)

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

first-party cookie (*témoins internes (de premier niveau)*)

A cookie is a data file sent by a web server to the web browser on a visitor's computer that the web server uses to track or record visitor information. First-party cookies are those cookies set by the website the visitor is visiting.

flow of personal information (*flux des renseignements personnels*)

Describes the creation, collection, retention, use, disclosure and disposition of personal information. It also includes the identification of partners that handle the personal information during the administration of a program or an activity.

handling (*traitement*)

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

indirect collection (*collecte indirecte*)

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

information-sharing agreement (*accord d'échange de renseignements*)

A written record of understanding that outlines the terms and conditions under which personal information is disclosed between parties. An information-sharing agreement is usually employed to facilitate the disclosure of personal information from a federal institution to a public sector entity external to the Crown. An information-sharing agreement may or may not be legally binding.

information-sharing arrangement (*entente d'échange de renseignements*)

A written record of understanding that outlines the terms and conditions under which personal information is disclosed between parties. An information-sharing arrangement is usually employed to facilitate the disclosure of personal information between and within federal institutions. An information-sharing arrangement is not legally binding.

information technology (*technologie de l'information*)

Any equipment or system that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of information or data. It includes all matters concerned with the design, development, installation and implementation of information systems and applications.

Internet Protocol address (*adresse du protocole Internet (IP)*)

A numerical label assigned by the Internet service provider to each computer. It is how the computer user communicates on the Internet. An Internet Protocol (IP) address may, in some circumstances, be linked with an identifiable individual whose computer is using that address at any given time. Therefore, the Government of Canada considers the IP address to be personal information that must, in all cases, be dealt with in accordance with the requirements of the Act.

internet service provider (*fournisseur de services Internet*)

An organization that provides access to the Internet.

lead government institution (*institution fédérale responsable*)

The government institution that leads the multi-institutional privacy impact assessment (PIA) and that is responsible for determining the most appropriate approach for the completion and approval of the PIA in support of a multi-institutional program or activity.

official responsible for section 10 of the *Privacy Act* (*agent responsable pour l'article 10 de la Loi sur la protection des renseignements personnels*)

The officer(s) or employee(s) who have been designated through a delegation order with the responsibilities of the head or the officer(s) or employee(s) who performs those responsibilities in the name of the head with respect to section 10 of the *Privacy Act*, which concerns the establishment of personal information banks for the personal information under the control of the government institution.

original purpose (*fin originale*)

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 (*mesures de protection physique*)

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

predominantly (*principalement*)

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 notice (*avis de confidentialité*)

A verbal or written notice informing an individual of the purpose of collecting their personal information as well as the government institution's legal authority for the collection. The notice, which must reference the PIB described in *Info Source*, also informs the individual of how their personal information will be used and disclosed, their right to access and request the correction of the personal information, any consequences of refusing to provide the information requested, and their right to file a complaint to the Privacy Commissioner of Canada.

privacy practices (*pratiques relatives à protection de la vie privée*)

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

Regulatory Impact Analysis Statement (RIAS) (*résumé de l'étude d'impact de la réglementation (REIR)*)

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 (*source fiable*)

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.

substantial modification (*modification importante*)

Refers to a change to the practices of an operating program or activity with respect to the creation, collection, retention, accuracy, correction, use, disclosure and disposal of personal information.

technical safeguards (*mesures de protection technique*)

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

web analytics (*Web analytique*)

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: Mandatory Procedures for Privacy Breaches

B.1 Effective date

- B.1.1 These mandatory procedures take effect on March 1, 2024.
- B.1.2 These mandatory procedures replace the Mandatory Procedures for Privacy Breaches dated October 26, 2022.

B.2 Procedures

- B.2.1 These mandatory procedures for privacy breaches provide details on the requirements set out in section 4 of the *Directive on Privacy Practices*.

B.2.2 Employees of government institutions must:

B.2.2.1 Take immediate measures to contain any potential or confirmed privacy breach and secure the affected personal information; and

B.2.2.2 Once any containment measures have been taken, immediately notify the head of the institution or their delegate of the potential or confirmed privacy breach. The notification is to include:

B.2.2.2.1 The date, time and location of the potential or confirmed privacy breach; and

B.2.2.2.2 A brief description of the potential or confirmed privacy breach, including the type of personal information affected and the number of individuals potentially affected, and any containment measures taken.

B.2.3 Executives and senior officials who manage programs or activities that involve the creation, collection or handling of personal information must:

B.2.3.1 If personal information affected by a privacy breach is the subject of a contract, information-sharing agreement or information-sharing arrangement, promptly notify the parties to that

contract, information-sharing agreement or information-sharing arrangement;

- B.2.3.2 If a full assessment of the breach is determined to be required by the head of the government institution or their delegate, ensure that an appropriate program official is assigned to coordinate with the head of the government institution or their delegate;
- B.2.3.3 In coordination with the head of the government institution or their delegate, determine appropriate mitigation measures to reduce the risks of harm to affected individuals and to the institution from the breach, which, in the event of a material privacy breach, must include notification of the affected individuals unless such notification would be inappropriate for security, confidentiality, legal or other reasons;
- B.2.3.4 In coordination with the head of the government institution or their delegate, determine appropriate prevention measures to reduce the risk of future breaches; and
- B.2.3.5 Enact the mitigation and prevention measures that are determined to be appropriate within a reasonable time frame.

B.2.4 Heads of government institutions or their delegates must:

- B.2.4.1 On receiving notification of a potential privacy breach, verify whether it does, in fact, constitute a privacy breach;
- B.2.4.2 In the event of a privacy breach, determine the need for a full assessment. A full assessment identifies and documents, at a minimum:
 - B.2.4.2.1 The circumstances that gave rise to the breach;
 - B.2.4.2.2 The inventory of personal information that was affected;
 - B.2.4.2.3 The individuals whose personal information was affected;
 - B.2.4.2.4 The institutional sectors and third parties, if any, who have a direct or indirect role in handling the personal information involved in the breach;
 - B.2.4.2.5 The risk of harm to individuals affected and to the institution; and
 - B.2.4.2.6 Whether the breach constitutes a material privacy breach;
- B.2.4.3 Collaborate as needed with institutional security officials, including those responsible for cyber security where appropriate, in any assessment of

the privacy breach or investigation of a related security event;

B.2.4.4 Include, at a minimum and where known, the following information when reporting a material privacy breach to the Office of the Privacy Commissioner (OPC) and to the Treasury Board of Canada Secretariat (TBS):

- B.2.4.4.1 The date of the breach or the period during which it occurred and the date on which the institution discovered the breach;
- B.2.4.4.2 A description of the breach, including its type and cause;
- B.2.4.4.3 The number or approximate number of individuals affected by the breach;
- B.2.4.4.4 The categories and elements of personal information involved;
- B.2.4.4.5 The parties involved, including the class of individuals affected by the breach and the relationships between the parties involved;
- B.2.4.4.6 A description of the relevant safeguards that were in place;

- B.2.4.4.7 The real risks of significant harm that are anticipated;
 - B.2.4.4.8 All remedial actions, including containment, mitigation and prevention measures, that were or will be taken;
 - B.2.4.4.9 The method used to notify individuals whose personal information was affected, if applicable; and
 - B.2.4.4.10 Justification should individuals whose personal information was affected not be notified;
 - B.2.4.4.11 The physical or geographic location where the breach occurred;
 - B.2.4.4.12 A description of how the breach was discovered;
 - B.2.4.4.13 The PIBs for the information subject to the breach, if applicable; and
 - B.2.4.4.14 A list of any organizations that were notified of the breach.
- B.2.4.5 When reporting a material privacy breach to the OPC and TBS, use the following means:
- B.2.4.5.1 The *Privacy Act* Material Privacy Breach form

- B.2.4.6** Maintain a record of all privacy breaches for a period of five years after the date the institution became aware of the breach. The record must include, at a minimum:
- B.2.4.6.1** The date of the breach or the period during which it occurred;
 - B.2.4.6.2** A general description of the circumstances of the breach and the nature of the information involved;
 - B.2.4.6.3** The full assessment of the breach if one was undertaken; and
 - B.2.4.6.4** In the case of a material privacy breach, the information provided to the OPC and TBS as prescribed by subsection B.2.4.4.

Appendix C: Standard on Privacy Impact Assessment

C.1 Effective date

- C.1.1** This standard takes effect on October 9, 2024.
- C.1.2** This standard applies to all programs and activities that involve the creation, collection, use, disclosure, retention or disposal of personal information. However,

- C.1.2.1 Institutions will have until October 10, 2025, to meet the requirements in subsections C.2.2.1.2 and C.2.2.9.4 of this standard.

C.2 Standards

- C.2.1 This standard provides details on the requirements set out in section 4 of the *Directive on Privacy Practices*.
- C.2.2 Standards are as follows:

Personal information banks

- C.2.2.1 Prepare a personal information bank (PIB):
- C.2.2.1.1 Prior to undertaking a new program or activity that uses personal information:
 - C.2.2.1.1.1 For an administrative purpose; or
 - C.2.2.1.1.2 Where the personal information is organized and retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual; and

C.2.2.1.2 When there is no PIB for an existing program or activity that uses personal information:

C.2.2.1.2.1 For an administrative purpose; or

C.2.2.1.2.2 Where the personal information is organized and retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

C.2.2.2 Update an existing PIB when:

C.2.2.2.1 Substantial modifications are to be made to the program or activity; or

C.2.2.2.2 Editorial changes or corrections are to be made to the PIB.

C.2.2.3 Terminate a PIB when confirmation is received that the records or personal information referred to in the PIB have been disposed of in accordance with the institution's Records Disposition Authority and are no longer under the control of the institution.

C.2.2.4 To register, update, transfer or terminate a PIB:

- C.2.2.4.1 Submit a request to the Treasury Board of Canada Secretariat (TBS);
 - C.2.2.4.2 Consider and respond to recommendations from TBS;
 - C.2.2.4.3 Obtain the approval of the President of the Treasury Board unless otherwise specified in the terms and conditions of a delegation under subsection 71(6) of the *Privacy Act*; and
 - C.2.2.4.4 Update the TBS-prescribed repository for new, substantially modified, edited or terminated personal information banks.
- C.2.2.5 When preparing, updating, transferring or terminating a PIB, use the following means:
- C.2.2.5.1 The Personal Information Bank Submission form, see [Treasury Board of Canada Secretariat Forms](#) for more information.

Documentation

- C.2.2.6 Document decisions to initiate or update privacy impact assessments (PIAs), multi-institutional PIAs and privacy protocols:

- C.2.2.6.1 Prior to undertaking a new program or activity that could involve the creation, collection, use, disclosure, retention or disposal of personal information; or
- C.2.2.6.2 When the institution intends to substantially modify an existing program or activity;
- C.2.2.6.3 Using the following means:
 - C.2.2.6.3.1 The Privacy Checklist, see Treasury Board of Canada Secretariat Forms for more information.
- C.2.2.7 Obtain approval of the Privacy Checklist from:
 - C.2.2.7.1 The executive or senior official who manages the program or activity; and
 - C.2.2.7.2 The official responsible for section 10 of the *Privacy Act*.
- C.2.2.8 Prior to initiating a PIA that involves more than one institution, provide a copy of the approved Privacy Checklist to TBS and the Office of the Privacy Commissioner (OPC), while respecting Cabinet confidences.

Privacy impact assessments

- C.2.2.9 Complete a PIA or update an existing PIA:

- C.2.2.9.1 Prior to undertaking a new program or activity that will involve the creation, collection, use, disclosure, retention or disposal of personal information for an administrative purpose;
- C.2.2.9.2 When substantial modifications are to be made to an existing program or activity that uses personal information for an administrative purpose, including through:
 - C.2.2.9.2.1 The use of any new or modified information technology or other process;
 - C.2.2.9.2.2 The involvement of any other institution or any third party under contract, agreement or arrangement with the institution;
 - C.2.2.9.2.3 The use of an automated decision system that would require compliance with the *Directive on Automated Decision-Making*; or

- C.2.2.9.3 When the official responsible for section 10 of the *Privacy Act* determines that a PIA is warranted given the potential risks associated with any administrative or non-administrative use of personal information; or
- C.2.2.9.4 When an existing program or activity that uses personal information for an administrative purpose does not already have a PIB;
- C.2.2.10 When initiating a multi-institutional PIA, appoint a lead institution for the completion of the PIA.
- C.2.2.11 When completing or updating an existing PIA, using the following means:
 - C.2.2.11.1 The Privacy Impact Assessment template, see Treasury Board of Canada Secretariat Forms for more information.
- C.2.2.12 Provide to TBS and the OPC:
 - C.2.2.12.1 All completed PIAs; and
 - C.2.2.12.2 Any information related to a PIA requested by TBS or the OPC, while respecting Cabinet confidences.

- C.2.2.13 Consider and respond to recommendations from TBS and the OPC related to a PIA.
- C.2.2.14 Obtain approval of the PIA from the executive or senior official who manages the program or activity and the official responsible for section 10 of the *Privacy Act*.
- C.2.2.15 Following the approval of the PIA, publish a summary that respects security, confidentiality and legal requirements, using the following means:
 - C.2.2.15.1 Summary of the Privacy Impact Assessment (Web Summary), see [Treasury Board of Canada Secretariat Forms](#) for more information.
- C.2.2.16 Implement the risk mitigation measures identified in the PIA.
- C.2.2.17 Review and update the risk mitigation measures identified in the PIA annually or as risks are mitigated.

Privacy protocols

- C.2.2.18 Complete or update a privacy protocol when a program or activity involves the creation, collection, use, disclosure, retention or disposal of personal information for a non-administrative purpose.

- C.2.2.19 When completing a privacy protocol, document the following at a minimum:
- C.2.2.19.1 The name of the program or activity;
 - C.2.2.19.2 The name and contact information of the official responsible for the program or activity;
 - C.2.2.19.3 A description of the program or activity;
 - C.2.2.19.4 The purpose for the collection of the personal information;
 - C.2.2.19.5 The legal authority for the collection of personal information;
 - C.2.2.19.6 The elements of personal information being collected as part of the program or activity;
 - C.2.2.19.7 Whether proper notification was given for the collection of personal information;
 - C.2.2.19.8 Whether personal information will be disclosed, and if so:
 - C.2.2.19.8.1 The purpose for the disclosure of personal information; and

C.2.2.19.8.2 The legal authority to disclose personal information;

C.2.2.19.9 The safeguards in place to protect the personal information; and

C.2.2.19.10 The retention and disposal standards that will apply to the program or activity.

C.2.2.20 Obtain approval of the privacy protocol from the executive or senior official who manages the program or activity and the official responsible for section 10 of the *Privacy Act*.

C.2.2.21 When registering, modifying or transferring a PIB for a program or activity that uses personal information for a non-administrative purpose, provide to TBS and the OPC:

C.2.2.21.1 The approved privacy protocol for the program or activity; and

C.2.2.21.2 Any information related to the privacy protocol requested by TBS or the OPC, while respecting Cabinet confidences.

C.2.2.22 Consider and respond to recommendations from TBS or OPC related to privacy protocols.

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

- D.1 Under paragraph 8(2)(e) of the *Privacy Act* (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.
- D.2 Requirements related to paragraph 8(2)(e) of the Act are as follows:

Requests under paragraph 8(2)(e)

- D.2.1 Requests made under paragraph 8(2)(e) of the Act are to be in writing and are to contain:
- D.2.1.1 The name of the investigative body;
 - D.2.1.2 The name of the individual who is the subject of the request or some other personal identifier;
 - D.2.1.3 The purpose of the request and a description of the information to be disclosed;
 - D.2.1.4 The section of the federal or provincial statute under which the investigative activity is being undertaken; and

D.2.1.5 The name, title and signature of the member of the investigative body who is filing the request.

D.2.2 All copies of such requests received by an institution are to be retained.

Documenting 8(2)(e) disclosures

D.2.3 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:

D.2.3.1 Clear indication as to whether the request was granted or refused;

D.2.3.2 The date the request was received;

D.2.3.3 The PIBs in which the disclosed information is held;

D.2.3.4 The specific personal information, record or file that was disclosed;

D.2.3.5 The name, title and signature of the official who authorized the response; and

D.2.3.6 The name of the investigative body that made the request.

D.2.4 A separate personal information bank (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.

Appendix E: Standard on Privacy in Web Analytics

E.1 Effective date

- E.1.1 This standard takes effect on October 26, 2022.
- E.1.2 This standard replaces the *Standard on Privacy and Web Analytics* (January 31, 2013).

E.2 Standards

- E.2.1 This standard provides details on the requirements set out in section 4 of the *Directive on Privacy Practices* as they pertain to web analytics.
- E.2.2 Heads of government institutions or their delegates are responsible for the following standards:
 - E.2.2.1 Information collected for web analytics that can be used to distinguish or trace an individual's identity, either alone or when combined with other identifying information that is linked or linkable to a specific individual, is considered personal information and is safeguarded in

accordance with the requirements of the *Privacy Act* (the Act).

- E.2.2.2 A privacy notice is provided on the institution's website that includes the following elements:
 - E.2.2.2.1 An explanation of what web analytics is and the purposes for its use by the institution;
 - E.2.2.2.2 A statement as to what specific personal information, including the Internet Protocol (IP) address, is being automatically collected from visitors by the government institution;
 - E.2.2.2.3 A statement setting out the legal authority for the collection of this information;
 - E.2.2.2.4 A statement advising visitors as to whether the IP address and other data in digital markers is being collected and used internally by the institution for the purpose of web analytics or is being disclosed or transmitted externally to a third party for that purpose;
 - E.2.2.2.5 In cases where the IP address and other data in digital markers are disclosed or transmitted to a third

party, an explanation of how the privacy of visitors to Government of Canada websites is being safeguarded through, at a minimum, the activation of the feature of third-party tools used for web analytics by which IP addresses are de-identified;

E.2.2.2.6 If data disclosed or transmitted for web analytics is going outside of Canada, a statement to that effect along with a reference to any governing legislation that the information might be subject to; and

E.2.2.2.7 A statement identifying the maximum retention period and the method of disposal for any personal information collected in relation to web analytics.

E.2.2.3 Any contract put in place for the purpose of web analytics must contain, in addition to the requirements outlined in subsection 4.2.34 of the *Directive on Privacy Practices*, at a minimum, the following provisions:

E.2.2.3.1 A definition of “personal information” as meaning information collected or generated in the performance of the contract about an individual, including the types of information specifically

described in the Act and also including information that may be linked or is linkable to an individual, such as the website visitor's IP address;

- E.2.2.3.2 A requirement that the third party appoint an officer within the organization to act as representative for all matters related to the personal information in question and that the name and contact information for this third-party contact be provided to the government institution within 10 days of the awarding of the contract;
- E.2.2.3.3 A requirement that the third party inform all of its employees, contractors and subcontractors of their privacy obligations when dealing with personal information disclosed or transmitted in relation to the work being performed under the contract or subcontract (the "work");
- E.2.2.3.4 A requirement that the third party de-identify the IP address prior to its storage in order that the full IP address cannot be reconstituted. This must be done through irrevocable truncation of the last octet of the IP address or

through some other methodology that offers comparable privacy protection and has been approved by the Treasury Board of Canada Secretariat (TBS);

- E.2.2.3.5 A requirement that the third party not link, or attempt to link, the IP address or some unique identifier associated with a digital marker with the identity of the individual computer user;
- E.2.2.3.6 A requirement that the de-identified IP address, along with other data disclosed to the third party for web analytics, be used only in accordance with the work, and that no subsequent uses or reuses of such data for any other purpose be allowed without the institution's express prior written authorization;
- E.2.2.3.7 A requirement that the third party not disclose or transfer the de-identified IP address or any other data disclosed to it except in accordance with the work, with the express prior written authorization of the institution, or if required to do so by law;

- E.2.2.3.8 A requirement that the third party use only first-party cookies;
- E.2.2.3.9 A requirement that the third party be prohibited from using techniques that raise the risk of identification, re-identification or profiling, such as but not limited to interlinking, cross-referencing, data mining or data matching from multiple sources on the personal information collected in relation to the work, unless expressly pre-authorized to do so, in writing, by the government institution;
- E.2.2.3.10 A requirement that the third party has security in place for the personal and de-identified information that is at least commensurate with the *Policy on Government Security*;
- E.2.2.3.11 A requirement that the third party safeguard the de-identified IP address and other information disclosed in relation to the work, and that this information be retained for a maximum period of six months, after which time the information, including any backup copies, must be destroyed; and

E.2.2.3.12 An audit provision whereby the third party may be audited at least once annually, at a date to be determined by the Government of Canada, to ensure compliance with these requirements.

E.2.3 Those authorized to perform web analytics on institutional servers or on servers hosted by third parties are responsible for the following standards:

E.2.3.1 The feature of third-party tools used for web analytics by which IP addresses are de-identified is activated;

E.2.3.2 Personal information is used only for the purpose of analytics; or a purpose for which the information may be disclosed by the institution under subsection 8(2) of the Act;

E.2.3.3 Personal information collected for the purpose of web analytics is not used for the following:

E.2.3.3.1 An administrative purpose, as defined in the Act, except where authorized to do so by law; and

E.2.3.3.2 To profile identifiable individuals, which includes producing inferences or other derivations from the personal information;

- E.2.3.4 The IP address and any other personal information, including but not limited to information in digital markers used in relation to web analytics, is safeguarded in accordance with the principles set out in subsection 4.3 of the *Directive on Service and Digital*; and
- E.2.3.5 The IP address and any other personal information, including but not limited to information in digital markers used in relation to web analytics, is retained for a maximum period of 18 months, after which time the information is disposed of in accordance with subsections 4.2.42 and 4.2.45 of the *Directive on Privacy Practices* and as authorized by the Librarian and Archivist of Canada.

© His Majesty the King in right of Canada, represented by the President of the Treasury Board, 2024,
ISBN: 978-0-660-73715-7

Date modified: 2024-11-08