



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Canada

Policy on Privacy Protection

Published: 2024-09-30

© His Majesty the King in Right of Canada,
represented by the President of the Treasury Board 2024,

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

Catalogue Number: BT39-24/2024E-PDF
ISBN: 978-0-660-73660-0

This document is available on the Government of Canada website, [Canada.ca](https://www.canada.ca)

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Politique sur la protection de la vie privée

Policy on Privacy Protection

1. Effective date

- 1.1 This policy takes effect on October 9, 2024.
- 1.2 This policy replaces the *Policy on Privacy Protection* dated October 26, 2022.

2. Authorities

- 2.1 This policy is issued pursuant to paragraph 71(1)(d) of the *Privacy Act* (the Act). This policy also contains elements that relate to paragraphs 71(1)(b) and (e) of the Act.
- 2.2 The President of the Treasury Board, as designated Minister for the paragraphs of the Act referenced in section 2.1 above, is responsible for establishing policies and prescribing forms concerning the operation of the Act and its Regulations.

3. Objectives and expected results

- 3.1 The objectives of this policy are as follows:
 - 3.1.1 Canadians have confidence that the government is protecting their privacy with regard to their personal information;
 - 3.1.2 Canadians have confidence that they can access their personal information that is under the control of government institutions;
 - 3.1.3 Personal information under the control of government institutions is effectively protected and managed through identifying, assessing, monitoring and mitigating privacy risks in programs and activities involving the collection, creation, retention, use, disclosure and disposal of personal information;
 - 3.1.4 Government institutions are accountable and transparent in the protection and management of personal information and in their response to privacy breaches; and
 - 3.1.5 Privacy considerations are incorporated into programs or activities at the design stage and are integrated into the governance and administration of programs involving the creation, collection, retention, use, disclosure and disposal of personal information.
- 3.2 The expected results of this policy are as follows:
 - 3.2.1 Government institutions have appropriate processes and tools to support the administration of the Act;

- 3.2.2 Government institutions offer requesters easily accessible mechanisms to make personal information requests;
- 3.2.3 Government institutions provide complete, accurate and timely responses to requests for personal information or correction of personal information;
- 3.2.4 Employees understand their obligations under the Act; and
- 3.2.5 Performance is measured, and compliance issues are identified and addressed.

4. Requirements

- 4.1 Heads of government institutions are responsible for the following:

Delegation of powers, duties and functions under the *Privacy Act*

- 4.1.1 Deciding whether to delegate, pursuant to section 73 of the Act, any of the powers, duties or functions under the Act that are listed in Appendix B: Powers That Can Be Delegated;
- 4.1.2 When signing a delegation order, giving careful consideration to the delegation of any powers, duties or functions pursuant to section 73 of the Act and ensuring that:
 - 4.1.2.1 Powers, duties and functions are:
 - 4.1.2.1.1 Delegated only to officers and employees of their government institution or of another government institution within the same ministerial portfolio when there is a service-sharing agreement between the two government institutions;
 - 4.1.2.1.2 Not delegated to consultants, members of a Minister's exempt staff, employees of other government institutions with which there is no service-sharing agreement, or to individuals from the private sector; and
 - 4.1.2.1.3 Delegated to positions identified by title, not to individuals identified by name;
 - 4.1.2.2 Delegates understand that they are accountable for any decisions they make but that ultimate responsibility remains with the head of the government institution;
 - 4.1.2.3 Delegates are at the appropriate level to be able to fulfill the duties of their delegated authorities and are well informed of their responsibilities;
 - 4.1.2.4 Delegates cannot further delegate powers, duties and functions that have been delegated to them, although employees and consultants may

perform tasks in support of delegates' responsibilities; and

- 4.1.2.5 Delegation orders are reviewed when the circumstances surrounding the delegations have changed. A delegation order remains in force until it is replaced.

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

Privacy practices

Privacy awareness

- 4.2.1 Ensuring that employees of the government institution are aware of policies, procedures and legal responsibilities under the Act;

Notification of planned initiatives

- 4.2.2 Notifying the Treasury Board of Canada Secretariat (TBS) and the Office of the Privacy Commissioner of Canada (OPC) of any planned initiatives (legislation, regulations, policies or programs) that could relate to the Act or to any of its provisions, or that may have an impact on the privacy of individuals. This notification is to take place at a sufficiently early stage to permit TBS and the OPC to review and discuss the issues involved while respecting Cabinet confidences;

Use of the Social Insurance Number

- 4.2.3 Ensuring compliance with the specific terms and conditions related to the use of the Social Insurance Number and the specific restrictions regarding its collection, use and disclosure as set out in the *Directive on Social Insurance Number*;

Personal information banks

- 4.2.4 Ensuring that personal information banks (PIBs) are prepared and updated, as required by section 10 of the Act;
- 4.2.5 Obtaining the approval of the President of the Treasury Board to establish, modify or terminate a PIB, unless otherwise specified in the terms and conditions of a delegation under subsection 71(6) of the Act;
- 4.2.6 Ensuring that TBS is consulted on any proposal to establish or terminate an exempt bank; and
- 4.2.7 Ensuring that the TBS-prescribed repository of PIBs is updated for new, modified or terminated PIBs;

Privacy impact assessments

- 4.2.8 Ensuring that, when applicable, privacy impact assessments and multi-institutional privacy impact assessments are developed, maintained and summaries published;

Privacy protocol for non-administrative purposes

- 4.2.9 Ensuring that, when applicable, privacy protocols are developed and maintained;

Privacy breaches

- 4.2.10 Establishing plans to address privacy breaches that affect personal information under the control of the institution, including those that occur within third-party entities under contract, agreement or arrangement with the institution;
- 4.2.11 Conducting periodic reviews of established plans that address privacy breaches to ensure that they reflect best practices and guidance;
- 4.2.12 Reporting material privacy breaches to TBS and the OPC after making efforts to contain, assess and mitigate the breach and no later than seven days after the institution determines that the breach is material;
- 4.2.13 Notifying TBS of any potential or confirmed privacy breach that could affect multiple institutions;
- 4.2.14 Responding to direction, advice or information requests issued by TBS regarding a breach that affects multiple institutions; and
- 4.2.15 Being responsive to information requests from the OPC regarding privacy breaches;

Contracts, agreements and arrangements

- 4.2.16 Taking steps to ensure, when personal information is involved, that third parties under contract, agreement or arrangement with the government institution provide appropriate privacy protections;

Service sharing

- 4.2.17 Ensuring that the requirements of section 73.1 of the Act are respected when entering into a service-sharing agreement; and
- 4.2.18 Providing a copy of any new service-sharing agreement, and any material changes to an existing service-sharing agreement, to the President of the Treasury Board and to the Privacy Commissioner as soon as possible after entering into the agreement or after any material changes arise. This responsibility rests with the head of a government institution to which the services are provided;

Control of personal information

- 4.2.19 Determining, in a manner consistent with jurisprudence and considering any TBS guidance, whether the personal information is under the control of the government

Requests and corrections

Exercising discretion

- 4.2.20 Exercising discretion under the Act and associated regulations in a fair, reasonable and impartial manner with respect to decisions made in processing requests and resolving complaints pursuant to the Act;

Duty to assist: protecting the identity of the requester

- 4.2.21 Ensuring that requesters' identities are protected and used or disclosed only when authorized by the Act and where there is a clear need to know;

Duty to assist: complete, accurate and timely responses

- 4.2.22 Ensuring that every reasonable effort is made to assist requesters with the request in order to provide complete, accurate and timely responses;

Language of access

- 4.2.23 Providing the personal information in the official language requested, in accordance with subsection 17(2) of the Act;

Accessible format for requesters

- 4.2.24 Providing the personal information in an alternative format, in accordance with subsection 17(3) of the Act, when requested by the requester;

Processing requests

- 4.2.25 Establishing effective procedures and systems to respond to requests under the Act to ensure that:
- 4.2.25.1 Requests can be received through the prescribed platform in accordance with Appendix D: Prescribed Platforms for Receiving and Processing Personal Information Requests of the *Directive on Personal Information Requests and Correction of Personal Information* unless the institution has received an exception to use of the platform, and can be received in written format by other means;
 - 4.2.25.2 Requests are processed using prescribed platforms in accordance with Appendix D of the *Directive on Personal Information Requests and Correction of Personal Information* when platforms have been prescribed, unless the institution has received an exception to use the platform;

- 4.2.25.3 Deliberations and decisions concerning requests received under the Act are documented;
- 4.2.25.4 The requested personal information is reviewed to determine whether it is subject to the Act and, if it is, determining whether any exemptions apply;
- 4.2.25.5 The principle of severability is applied; and
- 4.2.25.6 Any consultations necessary for the processing of requests made pursuant to the Act are undertaken promptly.

Confidences of the King's Privy Council

- 4.2.26 Consulting the institution's legal counsel, consistent with established procedures, prior to excluding confidences of the King's Privy Council for Canada; and
- 4.2.27 Upon the request of the Privacy Commissioner, acquiring assurances that excluded information is a confidence of the King's Privy Council for Canada, consistent with established procedures;

Considering other means of making government information accessible

- 4.2.28 Establishing procedures to review the nature of requests received and assessing the feasibility of making frequently requested and disclosed types of information available by other means;

Monitoring and reporting

- 4.2.29 Monitoring compliance with this policy and its supporting instruments within their institution;
- 4.2.30 Investigating when issues regarding policy compliance arise and ensuring that appropriate remedial action is taken to address these issues;
- 4.2.31 Advising the Secretary of the Treasury Board on a timely basis when significant issues regarding policy compliance arise;
- 4.2.32 Preparing and tabling an annual report on the administration of the Act in each House of Parliament in accordance with requirements established by TBS;
- 4.2.33 Providing the OPC and TBS with a copy of the annual report;
- 4.2.34 Providing TBS with a statistical report on the administration of the Act within the institution; and
- 4.2.35 Providing the contact information of the appropriate officer to receive personal information or correction requests for publication in the prescribed contact list.

5. Roles of other government organizations

- 5.1 This section identifies other key government organizations in relation to this policy. 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 Issuing direction and guidance to government institutions with respect to the administration of the Act and the interpretation of this policy and its supporting instruments;
 - 5.2.2 Approving exceptions to any requirement in this policy or its supporting instruments;
 - 5.2.2.1 Advising the OPC of any exceptions to any requirement in this policy or its supporting instruments that have been granted that could relate to the Act or to any of its provisions, or that may have an impact on the privacy of Canadians;
 - 5.2.3 Prescribing forms and platforms to be used in the administration of the Act, as well as the form and content of the annual report to Parliament;
 - 5.2.4 Reviewing regularly, or at least every five years, this policy and its related directives, guidelines, forms and prescribed platforms to assess their continued effectiveness and accuracy. When substantiated by risk analysis, TBS will also ensure that an evaluation is conducted;
 - 5.2.5 Overseeing compliance with this policy and its supporting instruments across government institutions, leveraging existing reporting mechanisms as appropriate;
 - 5.2.6 Receiving and reviewing material privacy breach reports;
 - 5.2.7 Advising institutions on the management of multi-institutional privacy breaches that require a coordinated response;
 - 5.2.8 Designating the repository for PIBs for all new or modified PIBs;
 - 5.2.9 Publishing annually an index of personal information under the control of government institutions that is confirmed to be up to date;
 - 5.2.10 Reviewing new and modified PIBs and assigning a registration number to new PIBs; and
 - 5.2.11 Working with the Canada School of Public Service to integrate knowledge elements related to the Act and associated policy instruments into training courses, programs and knowledge assessment instruments.
- 5.3 The Privacy Commissioner of Canada is an Agent of Parliament with the duty of protecting and promoting privacy rights and is responsible for the following:

- 5.3.1 Receiving and independently investigating complaints from individuals or self-initiated complaints on any matter related to the handling of personal information by federal government institutions;
 - 5.3.2 Issuing findings and any recommendations that the Commissioner considers appropriate, in relation to investigations where a complaint is well founded, to the head of the government institution;
 - 5.3.3 Communicating the outcomes of investigations to the complainant;
 - 5.3.4 Receiving and reviewing material privacy breach reports;
 - 5.3.5 Conducting compliance reviews of the privacy practices of government institutions as the practices relate to the collection, retention, accuracy, use, disclosure and disposal of personal information by government institutions subject to the Act; and
 - 5.3.6 Reporting to Parliament on activities annually. The Privacy Commissioner can also report at any time on any important matter within the scope of the Commissioner's powers, duties and functions.
- 5.4 The Clerk of the Privy Council Office is responsible for ensuring the integrity of the Cabinet process and the stewardship of the documents that support this process. As custodian of the confidences of the King's Privy Council for Canada of the current and previous ministries, the Clerk is responsible for policies on the administration of these confidences and for the ultimate determination of what constitutes such confidences and must be consulted in a manner consistent with the guidance in the [Access to Information Manual](#).
- 5.5 The Department of Justice Canada is responsible for supporting the Minister of Justice in the role of designated Minister for certain provisions of the Act, specifically:
- 5.5.1 Designating, by order-in-council, the head of a government institution for the purposes of the Act;
 - 5.5.2 Recommending extensions of the right of access by order-in-council;
 - 5.5.3 Specifying in regulations the government institutions or part of a government institution for the purpose of paragraph (e) of the definition of personal information in section 3 of the Act;
 - 5.5.4 Specifying investigative bodies and classes of investigations;
 - 5.5.5 Specifying persons or bodies for the purposes of paragraph 8(2)(h);
 - 5.5.6 Specifying classes of investigations for the purpose of paragraph 22(3)(c); and
 - 5.5.7 Amending the Schedule of the Act.

6. Application

- 6.1 This policy and its supporting instruments apply to government institutions as defined in section 3 of the Act, including departments, ministries of state, any parent Crown corporations and any wholly owned subsidiary of these corporations.
- 6.2 This policy does not apply to the Bank of Canada.

7. Consequences of non-compliance

- 7.1 For government institutions that do not comply with this policy and its related instruments, there may be a requirement to provide additional information on the development and implementation of compliance strategies in their annual report to Parliament or to TBS directly. This reporting may be in addition to other reporting requirements.
- 7.2 TBS will work collaboratively with heads of institutions or their delegates to restore compliance.
- 7.3 On the basis of analysis of monitoring and information received, the President of the Treasury Board may make recommendations to the head of the government institution. Such recommendations could include that the additional information outlined in section 7.1 above be reported by the institution.
- 7.4 The President of the Treasury Board, upon notification by TBS officials of a systemic compliance issue at a government institution, may review and revoke any delegation made under subsection 71(6) of the Act. This provision allows the President of Treasury Board to delegate to heads of government institutions that are departments as defined in section 2 of the *Financial Administration Act* any of the powers, functions and duties of the President of the Treasury Board with regard to the review and approval of new or modified PIBs.

8. References

8.1 Legislation

- *Access to Information Act*
- *Access to Information Regulations*
- *Canada Evidence Act*
- *Canadian Charter of Rights and Freedoms*
- *Financial Administration Act*
- *Interpretation Act*
- *Library and Archives of Canada Act*
- *Official Languages Act*
- *Personal Information Protection and Electronic Documents Act*
- *Privacy Act*
- *Privacy Act Heads of Government Institutions Designation Order*
- *Privacy Regulations*

8.2 Related policy instruments

- [Directive on Identity Management](#)
- [Directive on Personal Information Requests and Correction of Personal Information](#)
- [Directive on Privacy Practices](#)
- [Directive on Security Management](#)
- [Directive on Service and Digital](#)
- [Directive on Social Insurance Number](#)
- [Directive on the Management of Procurement](#)
- [Policy on Access to Information](#)
- [Policy on Government Security](#)
- [Policy on People Management](#)
- [Policy on Service and Digital](#)
- [Policy on the Planning and Management of Investments](#)

8.3 Related guidance instruments and forms

- [Access to information and privacy implementation notices](#)
- [Access to Information Manual](#)
- [Delegation under the Access to Information Act and the Privacy Act](#)
- [Guidance on Preparing Information Sharing Agreements Involving Personal Information](#)
- [Info Source Online Publishing Requirements](#)
- [Privacy Breach Management Toolkit](#)
- [Supporting Tool for Access to Information and Personal Information Requests: Principles for Assisting Requesters](#)
- [Taking Privacy into Account Before Making Contracting Decisions](#)
- [The Digital Privacy Playbook](#)
- [Treasury Board of Canada Secretariat Forms](#)

9. Enquiries

- 9.1 Members of the public may contact questions@tbs-sct.gc.ca regarding any questions about this policy.
- 9.2 Employees of federal institutions may contact their [Access to Information and Privacy Coordinator](#) regarding any questions about this policy.
- 9.3 Access to Information and Privacy Coordinators may contact ippd-dpiprp@tbs-sct.gc.ca regarding any questions about this policy.

Appendix A: Definitions

Note: Certain terms contain excerpts (in quotation marks, with the reference cited) from the *Privacy Act* (the Act).

administrative purpose (*fins administratives*)

The use of personal information about an individual “in a decision-making process that directly affects that individual” (section 3). This includes all uses of personal information for confirming identity (that is, authentication and verification purposes) and for determining eligibility of individuals for government programs.

annual report (*rapport annuel*)

A report submitted by the head of a government institution to Parliament on the administration of the Act within the institution during the fiscal year.

complainant (*plaignant(e)*)

An individual who makes a complaint to the Privacy Commissioner on any of the grounds outlined in subsection 29(1) of the Act.

consistent use (*usage compatible*)

A use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the proposed purpose, even if the use is not spelled out.

data matching (*couplage des données*)

An activity involving the comparison of personal information from different sources, including sources within the same government institution, for administrative or non-administrative purposes. The data-matching activity that is established can be systematic or recurring. The data-matching activity can also be conducted on a periodic basis when deemed necessary. Under this policy, data matching includes the disclosure or sharing of personal information with another organization for data-matching purposes.

delegate (*délégué*)

An officer or employee of a government institution or of another government institution within the same ministerial portfolio when there is a service-sharing agreement between the two government institutions, who has been delegated to exercise or perform the powers, duties and functions of the head of the institution under the Act.

designated minister (*ministre désigné*)

A person who is designated as the Minister under subsection 3.1(1). For the purposes of this policy, the designated minister is the President of the Treasury Board.

disclosure (*communication*)

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

excluded information (*renseignements exclus*)

The information to which the Act does not apply, as described in sections 69, 69.1, 70 and 70.1.

exempt bank (*fichier inconsultable*)

A personal information bank that describes files, all of which consist predominantly of personal information that relates to international affairs, defence, law enforcement and investigation, as outlined in sections 21 and 22 of the Act. The head of a government institution can refuse to disclose any personal information requested that is contained in an exempt bank.

exemption (*exception*)

A mandatory or discretionary provision under the Act that authorizes the head of the government institution to refuse to disclose information in response to a request received under the Act.

government institution (*institution fédérale*)

Any department or ministry of state of the Government of Canada, or any body or office, listed in Schedule in the Act; any parent Crown corporation; and any wholly owned subsidiary of a Crown corporation, within the meaning of section 83 of the *Financial Administration Act*. The term “government institution” does not include Ministers’ offices.

head (*responsable*)

The member of the King’s Privy Council for Canada who presides over a department or ministry of state. In any other case, it is the person designated by the Act Heads of Government Institutions Designation Order. If no such person is designated, the chief executive officer of the government institution, whatever their title, is the head.

Info Source (*Info Source*)

The Treasury Board of Canada Secretariat–directed web page published by each government institution in which the institution describes their program responsibilities and information holdings, including personal information banks and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the Act. Data-matching activities, use of the Social Insurance Number and all activities for which privacy impact assessments were conducted must be cited in personal information banks, as applicable. The web page also provides contact information for government institutions as well as summaries of court cases and statistics on access requests. This web page must be updated at least once per year.

legal authority (*autorité légitime*)

Legal authority for a program or activity is usually contained in an Act of Parliament or subsequent Regulations. Approval of expenditures proposed in the Estimates and authorization by an Appropriation Act can be an indication of legal authority for a program or activity.

material privacy breach (*atteinte substantielle à la vie privée*)

A privacy breach that could reasonably be expected to create a real risk of significant harm to an individual. Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

multi-institutional privacy impact assessments (*évaluations des facteurs relatifs à la vie privée multi-institutionnelles*)

A privacy impact assessment that involves more than one government institution (see definition of “privacy impact assessment” below).

new consistent use (*nouvel usage compatible*)

A consistent use that was not originally identified in the relevant personal information bank description.

non-administrative purpose (*fins non-administratives*)

The use of personal information for a purpose that is not related to any decision-making process that directly affects the individual. This includes the use of personal information for research, statistical, audit and evaluation purposes.

personal information (*renseignements personnels*)

Information about an identifiable individual that is recorded in any form. See section 3 of the Act for additional information.

personal information bank (*fichier de renseignements personnels*)

A description of personal information that is organized or intended to be retrieved by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used or is available for an administrative purpose and is under the control of a government institution.

personal information request (*demande de renseignements personnels*)

A request for access to personal information under the Act.

privacy breach (*atteinte à la vie privée*)

The improper or unauthorized access to, creation, collection, use, disclosure, retention or disposal of personal information.

Privacy Commissioner (*commissaire à la protection de la vie privée*)

An Agent of Parliament appointed by the Governor in Council who is mandated to ensure that rights and obligations set out in the Act are respected.

privacy impact assessment (*évaluation des facteurs relatifs à la vie privée*)

A process prescribed in policy for identifying, assessing and mitigating privacy risks. Government institutions are to develop and maintain privacy impact assessments for all new or modified programs and activities that involve the use of personal information for an administrative purpose.

privacy implementation notice (*avis de mise en œuvre de la protection des renseignements personnels*)

A notice issued by TBS to provide guidance on the interpretation and application of the Act and its related policies, directives and guidelines.

privacy protocol (*protocole de protection des renseignements personnels*)

A description of a program or activity that involves the use of personal information for a non-administrative purpose. Privacy protocols are to be completed and updated to ensure that personal information is handled in a manner that is consistent with the principles of Act.

program or activity (*programme ou activité*)

An initiative that falls within the mandate of the government institution and that the institution has the legal authority to carry out. Also included in this definition are any activities conducted as part of the administration of the program or activity.

requester (*demandeur*)

A person who is requesting access to personal information about themselves or who has requested that a correction be made or a notation attached to their personal information.

severability (*prélèvement*)

Relates to the principle found under the *Access to Information Act* in which the protection of information from disclosure must be limited to the portions of information or material that the head of the government institution is authorized or obligated to refuse to disclose under the Act and should be applied as a best practice in the spirit of transparency.

social insurance number (*SIN*) (*numéro d'assurance sociale (NAS)*)

A number suitable for use as a file number or account number or for data-processing purposes, as defined in subsection 28.1(3) of the *Department of Employment and Social Development Act*. For the purposes of paragraph 3(c) of the Act, the SIN is an identifying number and is therefore considered to be personal information.

statistical report (*rapport statistique*)

Provides data on the administration of the Act in the previous fiscal year. The statistical report is included in government institutions' annual reports to Parliament. The forms used for preparing the report are prescribed by the designated minister, as provided under paragraphs 71(1)(c) and (e) of the Act.

Appendix B: Powers That Can Be Delegated

Pursuant to section 73 of the *Privacy Act*, the head of a government institution may, by order, designate one or more officers or employees of that institution, or in the case of a service-sharing agreement, employees of another government institution within the same ministerial portfolio, who are at the appropriate level, to exercise or perform any of the powers, duties or functions that are to be exercised or performed by the institutional head under the following provisions of the Act and the *Privacy Regulations*:

Privacy Act

- 8(2)(j) Disclosure for research purposes
- 8(2)(m) Disclosure in the public interest or in the interest of the individual
- 8(4) Copies of requests under 8(2)(e) to be retained
- 8(5) Notice of disclosure under 8(2)(m)
- 9(1) Record of disclosures to be retained
- 9(4) Consistent uses
- 10 Personal information to be included in personal information banks
- 14 Notice where access requested
- 15 Extension of time limits

- 16 Where access is refused
- 17(2)(b) Language of access
- 17(3)(b) Access to personal information in alternative format
- 18(2) Exemption (exempt bank): Disclosure may be refused
- 19(1) Exemption: personal information obtained in confidence
- 19(2) Exemption: where authorized to disclose
- 20 Exemption: federal-provincial affairs
- 21 Exemption: international affairs and defence
- 22 Exemption: law enforcement and investigation
- 22.1 * Exemption: information obtained by Privacy Commissioner
- 22.2 * Exemption: Public Sector Integrity Commissioner
- 22.3 Exemption: *Public Servants Disclosure Protection Act*
- 22.4 * Exemption: Secretariat of National Security and Intelligence Committee of Parliamentarians
- 23 Exemption: security clearances
- 24 Exemption: individuals sentenced for an offence
- 25 Exemption: safety of individuals
- 26 Exemption: information about another individual
- 27 Exemption: protected information – solicitors, advocates and notaries
- 27.1 Exemption: protected information – patents and trademarks
- 28 Exemption: medical record
- 33(2) Right to make representation
- 35(4) Access to be given
- 51(2)(b) Special rules for hearings
- 72(1) Report to Parliament

Privacy Regulations

- 9 Reasonable facilities and time provided to examine personal information
- 11(2) Notification that correction to personal information has been made
- 11(4) Notification that correction to personal information has been refused
- 13(1) Disclosure of personal information relating to physical or mental health may be made to a qualified medical practitioner or psychologist for an opinion on whether to release information to the requester
- 14 Disclosure of personal information relating to physical or mental health may be made to a requester in the presence of a qualified medical practitioner or psychologist

Footnotes

*
– **Note:** The exemptions identified with a footnote may be claimed only by the institutions named in the provision.

Date modified: 2024-11-08