



BANK OF CANADA  
BANQUE DU CANADA

# Annual Report on the Administration of the *Privacy Act*

Published:

For the reporting period of April 1, 2024 – March 31, 2025

## Table of Contents

Introduction.....	1
Bank of Canada Mandate .....	1
Delegation and Organizational Structure.....	1
Performance 2024-2025.....	2
Formal Requests .....	2
Informal Requests.....	2
Consultations .....	2
Extensions .....	3
Complaints .....	3
Training and Awareness Program .....	3
Institution Specific Policies, Guidelines and Procedures .....	3
Initiatives and Projects to Improve Privacy.....	4
Material Privacy Breaches .....	4
Privacy Impact Assessments .....	5
Public Interest Disclosures.....	5
Monitoring Compliance .....	5
Annex A: Delegation of Authority.....	6



## Introduction

The *Privacy Act* (PA) gives individuals the right to access their own personal information held by federal government institutions, and protects that information against unauthorized collection, use, retention, and disclosure.

Access to Information, including personal information, is a quasi-constitutional right in Canada. The PA also enables individuals to exercise their privacy rights.

This report, prepared and tabled in accordance with Section 72 of the PA, describes the Bank of Canada's privacy activities for 2024-25.

The Bank is not reporting on behalf of any wholly owned subsidiaries or non-operational institutions. Similarly, the Bank does not provide any services related to privacy to any other institution per section 73.1 of the PA.

## Bank of Canada Mandate

The Bank of Canada is the nation's central bank. Our main role, as defined in the Bank of Canada Act, is "to promote the economic and financial welfare of Canada."

The Bank has five core functions:

- ❖ **Monetary policy** – to keep inflation low, stable and predictable
- ❖ **Financial system** – to promote safe, sound and efficient financial systems within Canada and internationally
- ❖ **Currency** – to design, issue and distribute Canada's bank notes
- ❖ **Funds management** – to act as fiscal agent for the Government of Canada, advising on and implementing its public debt and foreign exchange reserve strategies
- ❖ **Retail payments supervision** – to supervise payment service providers, building confidence in the safety and reliability of their services and helping protect users from specific risks

## Delegation and Organizational Structure

Under Section 71(2) of the PA, the Governor of the Bank of Canada undertakes the responsibilities of the designated Minister for the purposes of subsections 71(1)(a) and (d).

Responsibility for compliance with the requirements of the PA has been delegated by the Governor under Section 73 to the General Counsel and Corporate Secretary of the Bank, the Deputy Corporate Secretary and Senior Director Compliance (the Bank's Access to Information and Privacy Coordinator), and the ATIP Director.

A copy of the Bank's Delegation Order is available in [Annex A](#).

The Bank's Executive and Legal Services (ELS) Department is responsible for fulfilling the Bank's compliance obligations under the PA. The Privacy and Access Centre of Expertise (PACE), within ELS, is tasked with administering the Bank's Access to Information and Privacy (ATIP) program; it consists of 8 dedicated resources including policy specialists, analysts, leaders, and an administrator. The Bank uses

the services of external consultants as required.

The Bank also has a network of contacts within each department who are responsible for retrieving relevant records and providing advice about the sensitivity of information within the records to PACE. Privacy requests are treated with the highest discretion because of the care that must be taken when handling sensitive personal information. Information about privacy requests is therefore only shared on a need-to-know basis.

If PACE receives a formal request for information that is typically available to the individual through a direct channel, such as information related to the work of the Bank's Unclaimed Properties Office, PACE will coordinate a response to the requester, including through these other channels, as required.

## Performance 2024-2025

The following section sets out some statistical highlights from the Bank's Statistical Report on the PA.

### Formal Requests

The Bank of Canada received 16 new formal privacy requests in 2024–25.

- ❖ In addition, 1 request was carried forward from the previous reporting period, none were carried over from more than one reporting period.
- ❖ Together they represent a workload of 17 formal requests.
- ❖ 15 requests were completed, 10 of which were closed within legislated timelines representing a 66.7% completion rate for on-time requests.
- ❖ 4 requests were closed within 15 days, 2 within 30 days, 2 within 60 days, 5 within 120 days, 1 within 180 days, and 1 more than 365 days past the original due date.
- ❖ Closed requests involved the processing of 1,485 pages. 2 requests were disclosed in full, 7 requests were disclosed in part, no records existed for 3 requests, and 3 requests were abandoned.
- ❖ No audio or video records were processed for the requests completed in this reporting period.
- ❖ 2 requests were carried over to 2025 – 26 beyond legislated timelines. Section 2.1 of the supplemental statistical report provides a detailed break-down of carry-over data.
- ❖ The Bank endeavors to respect deadlines and routinely keeps requesters informed of the status of their requests. Requests that are completed beyond the legislated timelines are typically more complex, broad in scope, involve a large volume of records, the co-mingling of requester personal information with personal information of other individuals, and require numerous internal consultations.

### Informal Requests

The Bank received 3 informal requests during the 2024-25 reporting period.

- ❖ Of the 3 informal requests, all were closed during the reporting period.

### Consultations

The Bank did not receive or process any consultations from other institutions under the PA in 2024–25.

## Extensions

In 2024–25, the Bank took 7 extensions as meeting the original time limit of 30 days would unreasonably interfere with the institution's operations

## Complaints

The Bank received no notices of complaints per section 31 of the PA in 2024–25 and there were 0 complaints outstanding at the end of 2024-25.

## Training and Awareness Program

As employees of a federal institution, all Bank staff are responsible for upholding the principles of the PA and all staff need to be prepared to support the fulfillment of personal information requests in the course of their daily business. To promote awareness of their roles and responsibilities, all staff receive mandatory ATIP training through a virtual learning module as part of the Bank's onboarding process. In 2024-25, 330 employees completed the ATIP awareness module.

PACE has 3 e-learning modules which address the obligations of protecting personal information and the principles of the PA. All employees are required to complete a mandatory privacy module as part of the Bank's annual Code of Business Conduct and Ethics compliance certification process. In 2024-25, 2725 employees completed one of these e-learning modules.

In support of the Bank's data strategy, the Bank developed a comprehensive awareness module that explains the sensitivity of handling datasets that include, or are derived from, personally identifiable information. Completion of this module is mandatory for Bank staff that are granted access to sensitive data sets.

The promotion of privacy practices is supported through the PACE Hub which serves as an on-line and interactive resource center of information for any Bank staff who interact with personal information as part of their role at the Bank. The PACE Hub is regularly updated with current and topical privacy content.

PACE offers ad hoc virtual and in-person training and awareness sessions to Bank staff. These sessions focus on the administration of the PA, the Bank's privacy framework and risk management tools, best practices for managing personal information throughout its lifecycle, privacy breach awareness, and mandatory training for staff who engage with sensitive datasets. In support of the Bank's Artificial Intelligence (AI) adoption strategy, PACE delivered sessions focusing on key strategic privacy considerations with respect to AI technology. In this reporting period, the PACE Office delivered a series of formal presentations to leaders focused on personal information banks, artificial intelligence and privacy breach awareness for contract managers.

In 2024-25, the ATIP Office delivered 20 sessions to 282 participants across Bank departments.

## Institution Specific Policies, Guidelines and Procedures

As privacy experts for the institution, PACE has a responsibility to ensure that privacy considerations are factored into decision-making processes at the Bank.

PACE engages with all areas of the Bank during the annual planning exercise to identify initiatives that

will directly or indirectly involve creating, collecting, disclosing, or managing personal information.

In 2024-25, privacy specialists from PACE participated on various internal governance and working committees, providing input and timely feedback to key stakeholders about the Bank's information and data management policies and practices. This includes major Bank initiatives such as the development of the Bank's AI policy documents, development of privacy focused assessment tools, to support the adoption of Artificial Intelligence technology in a manner that is ethical and proactively considers and assesses privacy impacts.

The Bank has fully embraced the use of data to inform decision-making, by leveraging current data sets and acquiring new sources of data. PACE provides ongoing advice about how to protect privacy rights when that data contains personal information. Designated data owners and stewards are made aware of their responsibilities to adhere to the principles of the PA in the course of their daily business activities.

PACE collaborates closely with other disciplines throughout the Bank to ensure that outsourcing arrangements are in line with the requirements set out in the PA. In this reporting period, PACE actively participated in initiatives to refine and streamline the vendor vetting process to ensure that third parties undergo a robust assessment in line with the services they are delivering to the Bank.

PACE also contributed to the evolution of the Bank's integrated incident response procedures, ensuring that incidents are triaged immediately for potential privacy risks.

## Initiatives and Projects to Improve Privacy

PACE strives to make the delivery of privacy services as seamless as possible and regularly reviews processes for improvements. Work continued on the multi-year ATIP modernization project, including updates to the case management system as well as the addition of several new modules which will streamline processes. Work will be completed in the next reporting period.

To assist individuals with exercising their privacy rights, the Bank publishes an inventory of its information holdings on its website. This public inventory, known as *Info Source*, describes the Bank's functions, programs and activities, and their related classes of records and personal information banks (PIBs). The Bank modified 11 PIBs in 2024-25.

Through participation in the Bank's Accessibility Working Committee, PACE is actively engaged in the Bank's efforts to promote and facilitate accessibility for its staff and those making requests for information. In addition, to make ATIP services more inclusive and facilitate culturally appropriate services for Indigenous requesters, PACE staff participated in a dedicated awareness discussion with the Bank's Senior Indigenous and Equity, Diversity and Inclusion Specialist, and supported the Bank's Indigenous hiring program.

## Material Privacy Breaches

In this reporting period, the Bank notified the Office of the Privacy Commissioner (OPC) of one breach. A third-party vendor providing services to the Bank confirmed breach of privacy for some individuals some current and former Bank employees.

In addition to notifying the OPC, the Bank sent a series of communications to those individuals that the

Bank determined either were or might have been affected by the breach. The breach was thoroughly investigated, and procedures were enhanced to mitigate against future incidents. The breach investigation is complete.

## Privacy Impact Assessments

A privacy impact assessment (PIA) is an extensive formal privacy review used to assess and evaluate privacy, confidentiality or security risks associated with the collection, use disclosure, or retention of personal information, and to develop measures intended to mitigate and, wherever possible, eliminate identified risks. The Bank contracts third-party service providers to conduct its PIA assessments.

In 2024–25, the Bank completed 2 PIAs which involved:

- ❖ assessing employees' compliance with the Bank's Flexible Work Arrangements Policy
- ❖ assessing criteria for the possible disclosure of personal information to another federal government institution

Summaries of completed PIAs are available upon request.

## Public Interest Disclosures

There are limited and specific cases where personal information may be disclosed without the consent of the individual in question. These limited circumstances are outlined in section 8(2) of the PA. The Bank did not make any public interest disclosures under section 8(2)(e), 8(2)(m), or 8(5) of the PA in 2024-25.

## Monitoring Compliance

PACE proactively monitors a variety of information networks for any coming changes to legislation that might impact the Bank. This proactive approach allows the Bank to plan effectively and implement any necessary structural or operational changes in a timely manner to ensure the Bank's compliance.

PACE holds weekly meetings to discuss and closely monitor all active files and keep senior staff, such as the ATIP Director, informed of operations. These meetings help PACE to better manage heavy workloads and improve response times to external requesters and internal clients.

Senior management and the Board of Directors are briefed periodically on operational metrics and annually on the overall administration of the ATIP program.

Further, contracts with third parties clearly indicate that the Bank is subject to the ATIP legislation and obliges these entities to support the Bank in the fulfilment of requests made under these statutes, as required. Further the agreements set out the requirements for the secure and appropriate management of Bank information, including personal information under the Bank's control, by the third parties.

The Bank is committed to upholding the highest standards of personal and professional conduct. Annually, the Bank requires its employees to acknowledge their awareness of, and compliance with, the Code of Business Conduct and Ethics. Within the Code, the Bank recognizes and accepts its responsibility to provide any individual or corporation present in Canada a right of access to information contained in records under the Bank's control. Staff are reminded of their responsibilities regarding the management of corporate information and personal information and are required to acknowledge their responsibilities and obligations under the PA as part of this annual exercise.

## Annex A: Delegation of Authority



September 13, 2023

**To:** Steve Thomas  
General Counsel & Corporate Secretary

**From:** Tiff Macklem  
Governor


Lesley Ryan  
Deputy Corporate Secretary and Senior Director, Compliance  
Access to Information and Privacy Coordinator

**Subject:** Delegation of Authority under the Access to Information Act and the Privacy Act

The Governor of the Bank of Canada, pursuant to section 95(1) of the *Access to Information Act* and section 73(1) of the *Privacy Act*, hereby designates the persons holding the positions set out on the schedule hereto, or the persons occupying on an acting basis those positions, to exercise the powers and functions of the Governor as the head of a government institution, under the section of the *Act* set out in the schedule opposite each position.

### Schedule

Position	<i>Access to Information Act</i> and regulations	<i>Privacy Act</i> and regulations
General Counsel & Corporate Secretary	Full authority	Full authority
Deputy Corporate Secretary and Senior Director, Compliance/ Access to Information and Privacy Coordinator	Full authority	Full authority
Director ATIP	As set out in Appendix A	As set out in Appendix B

  
Governor Tiff Macklem

Oct 31, 2023  
(Date)



## Appendix A (Responsibility Delegated to Director ATIP — Access to Information Act)

Sections	Description
7	Respond to request for access within 30 days; give access or give notice
8	Transfer a request to the government institution with greater interest; give written notice of the transfer to the applicant
9	Extend time limits for responding to request and give notice to Information Commissioner of extension of over 30 days
10	Issue notice where access refused- the record does not exist, or where the institution does not indicate if the records exists or not the specific provisions for refusal if the record existed
11	Administer the collection of fees or waive fees
12(2)(b)	Decide whether to translate requested record(s)
12(3)(b)	Convert record(s) in an alternative format, when necessary and reasonable
13(1)	Shall refuse to disclose any record obtained in confidence from another government
13(2)	May disclose any record referred to in 13(1) if the other government consents to the disclosure or makes the information public
14	May refuse to disclose any record if reasonably injurious to the conduct of Federal-Provincial affairs
15	May refuse to disclose any record if reasonably injurious to international affairs and defence or the detection, prevention, or suppression of subversive or hostile activities
16	May refuse to disclose any record pertaining to law enforcement and investigations, to information that could reasonably be expected to facilitate the commission of an offence, to confidential information on policing services for provinces or municipalities
17	May refuse to disclose any record that could reasonably threaten the safety of individuals
18	May refuse to disclose any record that could reasonably be expected to be materially injurious to the economic interests of Canada
19(1)	Shall refuse to disclose any record that contains personal information as defined in section 3 of the <i>Privacy Act</i>
19(2)	May disclose personal information if: the individual consents; the information is publicly available; disclosure is in accordance with section 8 of the <i>Privacy Act</i>
20	Shall refuse to disclose any record that contains third party information
21	May refuse to disclose any record that contains information related to the operations of government: advice/recommendations; consultations/deliberations; plans for negotiations; plans related to management of personnel
22	May refuse to disclose any record that contains information relating to testing or auditing procedures
23	May refuse to disclose any record that contains information subject to solicitor-client privilege
24	Shall refuse to disclose any record that is subject to statutory prohibitions as set out in Schedule II
25	Shall sever any information that can be disclosed
26	May refuse to disclose any record on reasonable grounds that such material is to be published within a 90-day period or longer
27(4)	May extend the time limit for third party notification
28(4)	Disclose a record pertaining to Third Party following 20 days from the notice having been issued to a third party of the decision to disclose, unless the third party requests a review of the decision as per section 44
68	Deny any record that is excluded in the <i>Act</i> , including published material or material available for purchase by the public
69	Deny any record that is excluded in the <i>Act</i> that constitute confidences of the Queen's Privy Council for Canada

## Appendix B (Responsibility Delegated to Director ATIP — *Privacy Act*)

Sections	Description
8(2)(a)-(l)	Disclose personal information on the basis of the requirements of subsection 8(2)
8(4)	Retain a record of any disclosure made under 8(2)(e)
9(1)	Retain records of use of personal information
9(4)	Notify the Privacy Commissioner of consistent use of personal information and update index accordingly
10	Include personal information in personal information banks
14	Respond to request for access within 30 days; give access or give notice
15	Extend time limit for responding to request for access
16	Issue notice where access refused
17	Form of Access/Language of Access/Alternative format
19(1)	Shall refuse to disclose information obtained in confidence from another government or organization
19(2)	May disclose any information referred to in 19(1) if the other government or organization consents to the disclosure or makes the information public
20	May refuse to disclose information if injurious to the conduct of Federal-Provincial affairs
21	May refuse to disclose if injurious to international affairs and defence or preventing or suppressing subversive or hostile activities
22	May refuse to disclose information prepared by an investigative body, information injurious to the enforcement of a law, or information injurious to the security or penal institutions
23	May refuse to disclose information prepared by an investigative body for security clearances
25	May refuse to disclose information which could reasonably threaten the safety of individuals
26	May refuse to disclose information about another individual, and shall refuse to disclose such information where disclosure is prohibited under section 8
27	May refuse to disclose information subject to solicitor-client privilege
28	May refuse to disclose information relating to the individual's physical or mental health where disclosure contrary to the best interest of the individual
69	Deny any record that is excluded in the Act, including library or museum material preserved solely for public reference or exhibition purposes
70	Deny any record that is excluded in the Act that constitute confidences of the Queen's Privy Council for Canada

### Reference

---

#### *Extracts of the Access to Information Act (R.S.C., 1985, c. A-1)*

##### Delegation by head of government institution

**95 (1)** The head of a government institution may, by order, delegate any of their powers, duties, or functions under this Act to one or more officers or employees of that institution.

#### *Extracts of the Privacy Act (R.S.C., 1985, c. P-21)*

##### Delegation by head of government institution

**73 (1)** The head of a government institution may, by order, delegate any of their powers, duties, or functions under this Act to one or more officers or employees of that institution.