

Privacy Booklet 2025





Table of Contents

3	Our One Mission
4	About This Booklet
5	Our Commitment
6	Our Privacy Program
7	Pillar 1: Accountability and Governance
9	Pillar 2: Assessment
11	Pillar 3: Training and Awareness
12	Pillar 4: Consent and Responsible Handling of Personal Information
14	Pillar 5: Incident Management
15	Pillar 6: Third-Party Management
16	Pillar 7: Monitoring and Measurement
17	Our Performance in 2025
17	Questions or Comments?

Our One Mission

We exist to have a positive impact in people's lives.

By building long-term relationships with our clients, teams, shareholders and our community.

People first.

Why do we need a One Mission?

Our One Mission is aligned with our continued efforts to drive social and economic development. In response to changing trends in the banking industry, we've adopted a people-first approach that will help us achieve our objectives and boost our collaboration with stakeholders.

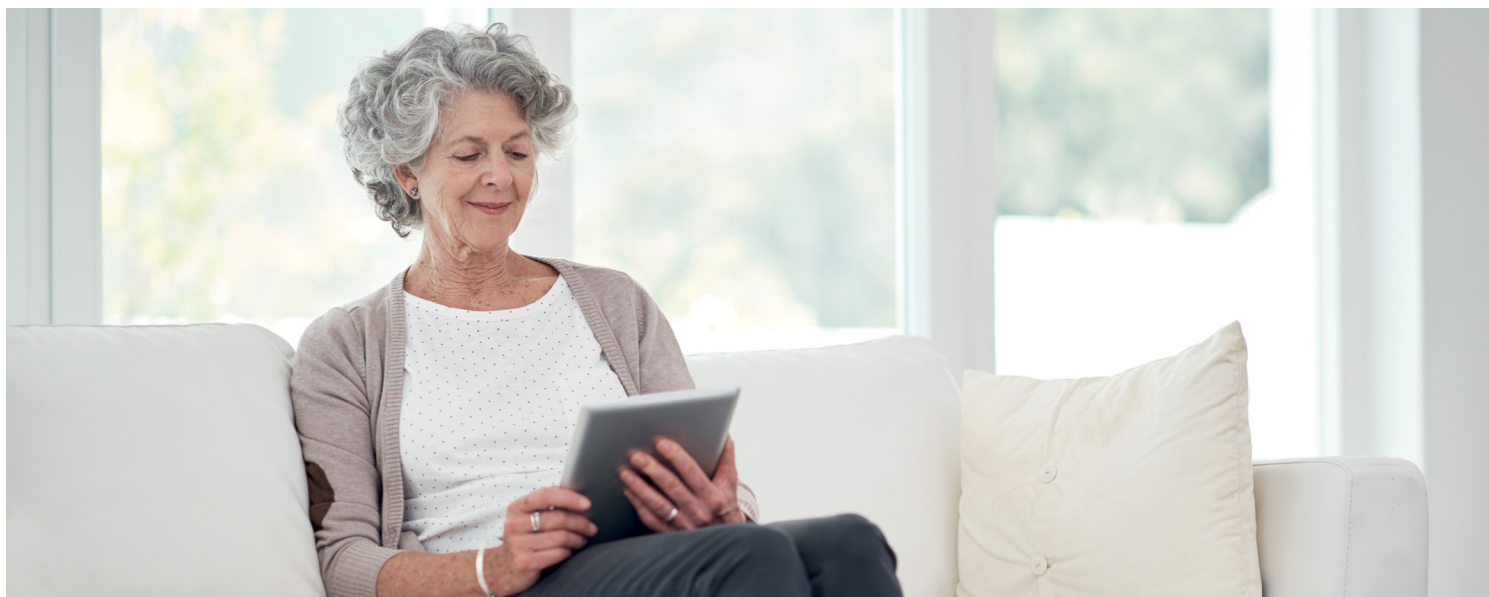
How is our One Mission put into practice?

- Through the experiences we want to deliver to our clients, our employees and the communities we serve.
- Through behaviours that reflect our values: partnership, empowerment and agility.
- Through the way employees work together to boost client satisfaction, employee engagement and community involvement.
- Through the initiatives we prioritize to have a positive impact.

About This Booklet

This booklet on **privacy** is produced by National Bank of Canada's Privacy and Responsible Artificial Intelligence Team (the Team). It demonstrates our commitment to building together on a foundation of trust and to using your personal information responsibly. This booklet also addresses the Team's role in developing our program to oversee the responsible use of artificial intelligence.

The protection of personal information is among the Bank's priorities. Over the years, measures have been put in place to reinforce our practices and earn your trust. These practices are set out in this booklet. We will keep you informed of any related progress and results on an annual basis.



Scope

The information in this booklet covers the activities of the Bank and its main Canadian subsidiaries⁽¹⁾ for the period from November 1, 2024, to October 31, 2025.

Who it is for: stakeholders

This booklet has been prepared to help our stakeholders understand our privacy program. It reflects our program, privacy practices, policies, standards and efforts in voluntary disclosure. This booklet aims to foster an ongoing dialogue between the Bank (including its directors and officers) and its clients, employees, shareholders and service providers as well as communities, interest groups and regulatory authorities.

This dialogue helps us enrich our practices and aim for the most advanced privacy and disclosure standards.

(1) The information provided in this report does not include Flinks Technology Inc.

Our Commitment

We do our utmost to ensure the protection of your personal information. All of our employees work together towards this goal.

Our commitment to you is simple: building together on a foundation of trust.

Our commitment is aligned with the Governance component of our Environmental, Social and Governance (ESG) principles, which have been approved by the Bank's Board of Directors. Our commitment to privacy contributes to advancing the United Nations Sustainable Development Goals, and in particular, goal 16: Peace, Justice and Strong Institutions. We have put in place a governance framework for the protection of personal information to ensure that we safeguard your data and maintain a relationship of trust with you.

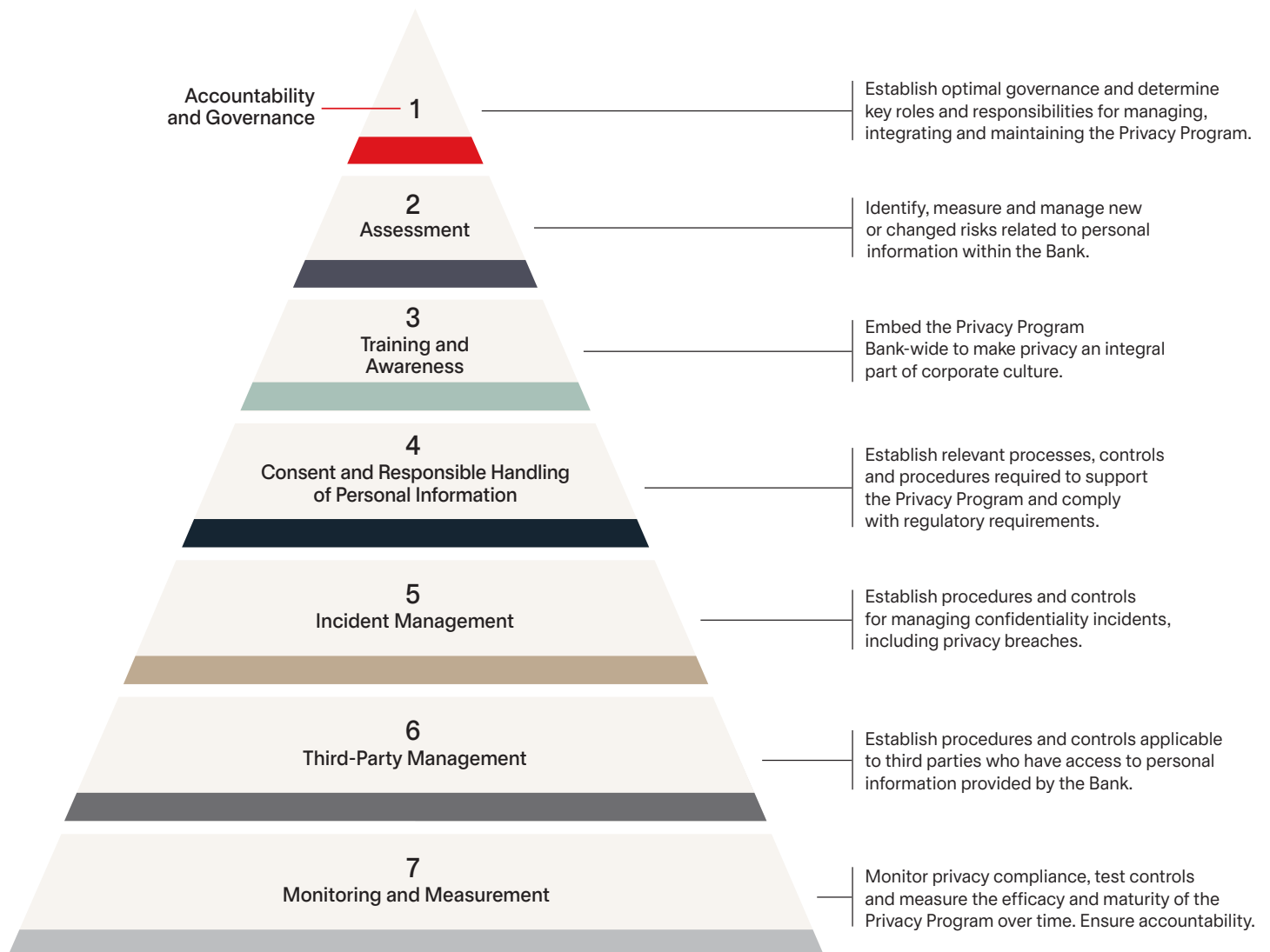
**Building together
on a foundation
of trust**

→ **RESPONSIBLE**
use of your
personal information

→ **SECURITY** measures
to protect your
personal information

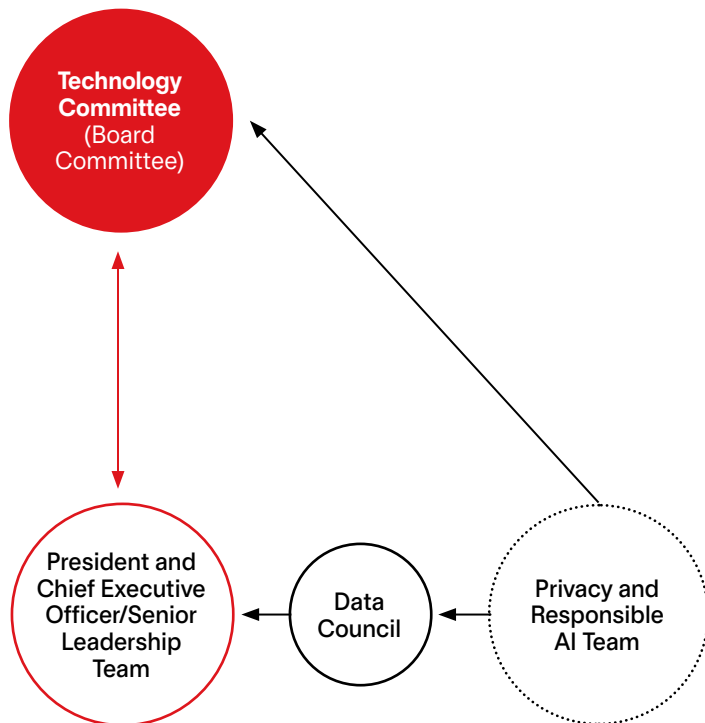
Our Privacy Program

The protection of personal information is crucial to accelerating our business model and strategies. Proper management of personal information helps preserve and strengthen this relationship of trust, creates value for our clients and organization, and reduces the risks associated with its processing. Our Privacy Program, which enables us to achieve these goals, is based on the following seven pillars:



Pillar 1: Accountability and Governance

We have adopted a robust governance framework that defines the roles and responsibilities of our various teams to ensure the management, integration and maintenance of our Privacy Program across the organization.



The Team's responsibilities also include:

- ensuring the protection and responsible handling of personal information, as well as compliance with applicable laws;
- supporting the Bank's business sectors in carrying out the adopted strategic orientations;
- proactively monitoring any new legislative requirements regarding the protection of personal information and responsible AI and ensuring compliance with best practices;
- analyzing emerging issues that may affect our internal practices and our commitments to you;
- making recommendations to various decision-making levels; and
- participating in the socialization of various reform initiatives related to privacy and responsible AI.

The Team periodically presents the various committees with:

- reports on privacy risks and the status of strategic initiatives; and
- new facts as well as emerging trends that may impact current practices.

Privacy and Responsible Artificial Intelligence Team (the Team)

The Team is headed by the Chief Privacy and Responsible Artificial Intelligence (AI) Officer, who reports to the Executive Vice-President and General Counsel, Enterprise Technology and Resilience.

The Team develops and implements our Privacy Program and privacy strategy. It is responsible for:

- the development, maintenance and implementation of policies, standards and procedures in support of our Privacy Program;
- the privacy risk governance framework; and
- recommending the establishment of appropriate risk mitigation controls.

Furthermore, the Team participates in the development and implementation of the responsible AI program. In this capacity, it collaborates on:

- developing policies, standards and procedures governing the responsible use of AI;
- assessing risks related to AI by establishing multidisciplinary evaluation processes;
- creating a multidisciplinary team to support and assist initiatives involving AI;
- establishing an accountability framework within the lifecycle of AI systems;
- developing an employee guide for the use of generative AI;
- integrating the eight principles of responsible AI into the design, development and deployment processes of AI systems: accountability, proportionality, fairness, security, reliability, explainability, transparency and protection of personal information; and
- developing an employee training program on best practices in responsible AI.

Pillar 1: Accountability and Governance (cont.)

The Board of Directors and the Technology Committee

The Bank's Board of Directors, through the Technology Committee, oversees the various components of the Bank's technology program. Among other things, it reviews the Bank's technology strategy and monitors technology risks, including cyber risks, cybercrime, privacy and the use of AI. The mandate and key achievements of the Board of Directors and the Technology Committee can be consulted in the relevant subsections of the [nbc.ca](https://www.nbc.ca) website devoted to governance and investors, under the "About Us" tab.

The Data Council

The Data Council is composed of Bank executives. Its mandate is to ensure the maximization of the business value of data, an important asset for the Bank. It has the authority to make decisions regarding how the Bank governs, manages and leverages business data under its responsibility (including personal information), while ensuring compliance with the policies, standards and practices that govern it and stem from the Bank's risk appetite framework.

The Executive Officers

The President and Chief Executive Officer and the senior leadership team approve the main strategic orientations and priorities relating to the protection of personal information. They are ambassadors within the organization and to the Bank's Board of Directors in relation to the protection of personal information.

Strengthening our Governance Through Privacy Champions

We are committed to creating a culture dedicated to protecting your personal information, one that resonates across all functions in our organization. In order to strengthen our governance, we have appointed "privacy champions" who support the Bank's initiatives involving personal information to leverage privacy in business strategies. They are, in a manner of speaking, the eyes and ears of the Privacy Team on the ground.

The role of the privacy champion is to:

- support business sectors with the development and implementation of projects and processes to ensure sound management of personal information;
- identify business issues as well as any awareness and training needs for the business sectors they support; and
- support business sectors when assessing privacy-related risks.

We are working to evolve the role of the privacy champions so that they can support business sectors in their responsible use of artificial intelligence and thereby strengthen our governance in this area.

Protecting Personal Information, a Shared Responsibility

The protection of personal information is the result of the collaboration and combined efforts of several business sectors and internal committees. Our personal information governance involves a **reporting process that enables** us to gauge the effectiveness of our practices so we can make decisions based on our commitment to you, our risk appetite and our ambition to offer you innovative products and solutions.

Pillar 2: Assessment

At the Bank, we have established processes to identify, assess and manage privacy risks, whether they are new or evolving. Our operational teams stay informed about privacy issues in their respective areas. They are also responsible for identifying, assessing and addressing privacy matters.

Ongoing Risk Assessments

The Privacy and Responsible Artificial Intelligence Team oversees several ongoing privacy risk assessments. For example, it supervises assessments concerning:

- the privacy risks associated with each sector of the Bank;
- the handling of privacy complaints;
- the management of privacy incidents; and
- the integration of third parties and vendors.

The Team ensures that privacy risks are consistently identified, assessed and managed within the organization.



Privacy Impact Assessments

The Bank has developed a rigorous process that allows it to assess privacy factors from the outset of its new initiatives or their updates. This process aims to ensure a clear understanding of privacy risks related to an initiative and to mitigate those risks. The process is completed by our operational teams, in collaboration with the privacy champions and the Privacy and Responsible Artificial Intelligence Team.

This process involves three steps:

- 1** A preliminary assessment of the initiative to determine its level of privacy risk.
- 2** Where required, a detailed assessment of the initiative's privacy impact and the identification of controls to mitigate the risks.
- 3** The implementation of the identified controls.

The Team ensures that privacy remains a central priority from the very inception of initiatives.

Pillar 2: Assessment (cont.)

Assessments of Cross-Border Data Movements

If it is necessary to move data across borders as part of our activities, we ensure compliance with applicable laws and best practices. A strict framework for cross-border data movements is in place, which includes:

- privacy impact assessments and risk analyses that consider the volume, sensitivity and intended use of the shared information; and
- assessment of recipient countries that consider the applicable legal regime and the broader legal and sociopolitical context.

These assessments are conducted to ensure that an adequate and comparable level of protection to that of the country of origin can be provided. When a third party is involved, third-party risk assessment processes are applied, including appropriate due diligence and the signing of robust contractual agreements.

Assessment of Fairness Factors

Technological transformations, especially those related to artificial intelligence and advanced analytics technologies, are drawing increasing attention. As an organization, we are mindful of the effects that these technologies can have on rights and freedoms as well as on our ability to positively transform the experience of our clients and employees.

We therefore proactively assess our practices to make sure that the technologies we deploy are aligned with our values. For example, our fairness by design program enables us to strengthen our responsible artificial intelligence and advanced analytics activities.

This cross-sector program provides for concrete measures that help reinforce best practices in equity. In this context, awareness and training activities were held within the different sectors of the Bank, for business development, supervisory and scientific teams as well as for employees of the second and third lines of defence. Performance indicators are in place to monitor our equity practices. For example, we track the effective adoption rate of the program by the analytical solutions that we have put into production in the last year.

Pillar 3: Training and Awareness

Our approach is as follows:

1. Mandatory training for new employees that makes them aware of the importance of privacy for the Bank and our clients, and equips them to protect it.
2. Annual mandatory privacy training, with a different theme each year to enhance employees' knowledge in this area.
3. Continuously raise awareness through training modules and activities to keep employees informed.
4. Targeted training to support certain business sectors—for example, when deploying a new initiative or improving processes.

Our goal is to have employees who are engaged and aware of the importance of protecting your personal information. Training is offered at all levels of our organization.

Training is updated periodically to meet new regulatory requirements and best practices. Our Code of Conduct also reinforces the importance of protecting personal information.



Mandatory Onboarding Training: NBC's Privacy Commitment

In 2025, this training was completed successfully by new employees. The completion rate for this mandatory onboarding training exceeds 99% annually.

2025 Mandatory Annual Training: Adopting Appropriate Behaviours for the Protection of Personal Information

95% of active employees completed the training.

In addition, the annual security training addressed the topic of privacy breaches, highlighting the associated risks and the preventive measures to adopt in response to such incidents.

Additionally, a training session on the use of generative artificial intelligence was completed by 97% of active employees and emphasized the importance of responsible use of personal information in this context.

Finally, the Privacy and Responsible Artificial Intelligence Team published short informational capsules on the Bank's internal social networks, covering topics of interest related to privacy and data protection.

Pillar 4: Consent and Responsible Handling of Personal Information

We develop and implement reliable processes to handle your personal information responsibly in accordance with your expectations and applicable laws.

How we uphold your rights throughout the life cycle of your personal information

Collection



Use



Communication



Retention



Destruction



- **Collection:** We limit the collection of your information to what is necessary to help us serve you properly.
- **Use:** We use your information in accordance with our Privacy Policy and our Digital Data Policy.
- **Communication:** At all times, we are committed to limiting the communication of your information to what is necessary.
- **Retention:** We retain your information for as long as necessary to fulfill the purposes for which the information was collected or as long as required or permitted by law. Our legal obligations, the purpose for collecting the information as well as the nature and the sensitivity of the information have been considered in determining retention periods. We have reviewed and simplified our retention periods to clarify the triggering event of the retention period.
- **Destruction:** When your information is no longer needed, we endeavour to securely destroy it.

The documentation we provide to you

In the spirit of transparency, we have published two policies that describe our practices related to the handling and protection of your personal information:

- [The Privacy Policy](#)
- [The Digital Data Policy](#)

We have developed these policies with you in mind. Your consent is the cornerstone of our practices; we respect your choices and act on the consent you have given.

Pillar 4: Consent and Responsible Handling of Personal Information (cont.)

Privacy Policy

This policy explains, among other things:

- what types of personal information we may collect and the reasons for collecting it;
- how we can use and share your information and with whom;
- the choice you have in consenting or not to certain uses of personal information; and
- our approach to protecting, retaining and destroying your personal information.

The policy also informs you about your rights to:

- access the personal information we have about you and request its disclosure;
- correct your personal information to ensure its accuracy;
- be informed when we make an exclusively automated decision about you (without human intervention), such as in response to certain credit or financing requests; and
- opt out of receiving our product and service offers and other promotional communications at any time.

Digital Data Policy

This policy explains, among other things:

- the types of information we collect using cookies and other similar technology;
- the purposes for which we collect this information; and
- your right to refuse and how to exercise it or change your preferences.

You have several simple options to communicate your concerns and complaints to us.

-
- To make a complaint, you must follow the procedures outlined on our website at [nbc.ca](https://www.nbc.ca), under **About us > Useful links > Complaint settlement online**.
-

Management of Individual Requests Regarding Personal Information

In general, when you make a request to access or correct your personal information, our employees respond as promptly as possible after authenticating your identity. If your request is complex or requires extensive searches in our systems, it will be forwarded to the Privacy Team. When the Privacy Team receives such a request, it makes the necessary efforts to conduct a thorough and complete search and respond within 30 days following your authentication. If you are not satisfied with the response received, you have recourse to the Office of the Privacy Commissioner of Canada or provincial privacy regulators, where applicable.

If you prefer to navigate online, our automated solution will allow you to quickly obtain the relevant personal information we hold about you, as well as details about your products and services at National Bank. To do so, log in to your online banking account, access your profile, select *Privacy Settings*, then choose *Request access* and follow the instructions. Your information will be placed in the secure document-sharing space, called My Document Exchange, within 30 days.

Complaint Management

The Bank wants to be transparent about how it manages your personal information, in addition to ensuring that it is handled responsibly. Any complaints relating to the protection of personal information are taken seriously. In order to quickly find solutions that suit you, the Bank has developed and maintains complaint-handling processes relating to the protection of personal information and trains its employees to manage privacy complaints in accordance with these procedures.

Our employees and the Privacy Team work together to answer your questions about the protection of your personal information, to guide you and to find solutions that are right for you.

Pillar 5: Incident Management



We make significant efforts to protect your personal information from loss, theft and unauthorized access, use or disclosure. We have practices in place that allow us to identify and fully understand our risks, as well as a security program in place to keep pace with changing information security threats. The measures adopted in our security program include:

- protecting our infrastructure through secure access to our premises and secure locations for our equipment, etc.;
- limiting who has access to your information, meaning that only employees who need to know your information in order to carry out their duties have access to it;
- managing passwords and setting up firewalls; and
- conducting security verifications at the time of hiring of all Bank employees.

If an incident were to occur and present a serious risk, you would be personally informed within the time limits provided by law. Additionally, the Bank would ensure that relevant regulators, as well as any individuals or organizations that could help reduce the risk of harm, are informed.

Pillar 6: Third-Party Management

Relationship With our Service Providers and Business Partners

The safety of your personal information is important, including when it must be shared with third parties. We take great care in choosing our business partners and service providers and have a third-party risk-management procurement process.

When it is necessary to use a service provider or a business partner who will hold information (including personal information) for which we are responsible, our process is applied and the elements related to the protection of personal information are integrated into all stages of the life cycle of a service provider or business partner.

The life cycle of a service provider or business partner

Assessment



Review



Agreement Negotiation



Agreement Management



Agreement Renewal



→ Under no circumstances do we sell client lists to third parties.

- **Materiality Assessment:** We perform a materiality assessment that includes privacy risk-related questions.
- **Due-Diligence Review:** We initiate a due-diligence process that includes a security and privacy review.
- **Negotiation of Agreements:** Our service providers or business partners may only use personal information in a responsible manner; they agree to use only the personal information required to provide their service and must be as diligent and cautious as we are to ensure the security of your personal information.
- **Agreement Management:** We ensure the right mechanisms are in place to monitor, among other things, compliance with security and privacy requirements. We also require that our service providers and business partners notify us of any privacy incidents so that we can work together to respond, remedy and, if applicable, report them.
- **Agreement Renewal, Expiry or Termination:** If we decide not to renew an agreement with our service provider or business partner, the Bank and its service provider or business partner comply with the relevant contractual clauses, in particular those relating to the retrieval and the destruction of personal information.

Pillar 7: Monitoring and Measurement

The Bank monitors its Privacy Program by testing certain controls and using metrics to assess their effectiveness over time.

Each business sector is responsible for monitoring the effectiveness of the controls in place to ensure the protection of personal information within its operations. The compliance sector also conducts independent oversight of the organization's practices to ensure they comply with privacy requirements.

Additionally, the Privacy Team identifies and monitors privacy-related laws and regulations and ensures the implementation of new requirements within the organization.



Our Performance in 2025

Our practices are evolving, and we are continuously improving our performance indicators to better assess the quality of our practices. Our goal is to improve the effectiveness of our strategies and operational processes.

We have implemented an indicator based on the number of decisions made annually by regulators regarding the Bank.

Decisions regarding
personal information
involving the Bank



Annual target
0



*Result in 2025
1

*The Commission d'accès à l'information du Québec ruled in favour of the Bank in a case reviewing a request for access to personal information, thereby confirming that the Bank had acted in compliance with applicable laws.

Questions or Comments?

Your feedback is important to us. We are committed to following up on it in a straightforward manner so you can understand how we handle your personal information.

If you have any questions or comments, please contact:

1 Your branch's Customer Service Manager

2 The Chief Privacy and Responsible Artificial Intelligence Officer at:
confidentiality@nbc.ca
or **National Bank Place**
800 Saint-Jacques Street
Montreal, Quebec, Canada H3C 1A3