NATIONAL BANK

Privacy Booklet

2022

Table of Contents

OUR ONE MISSION

We exist to have a **POSITIVE IMPACT** in people's lives.

By building ***long-term relationships*** with our clients, employees and communities.

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 (the Bank) Privacy Office. It is a testament to our commitment to being transparent and offering you an experience in line with your expectations.

Privacy is one of 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, 2021, to October 31, 2022.

Who it is for—stakeholders

This booklet has been prepared to help our stakeholders understand our privacy program. It reflects a summary of our program as well as our privacy practices, policies and standards and our voluntary disclosure efforts. 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.

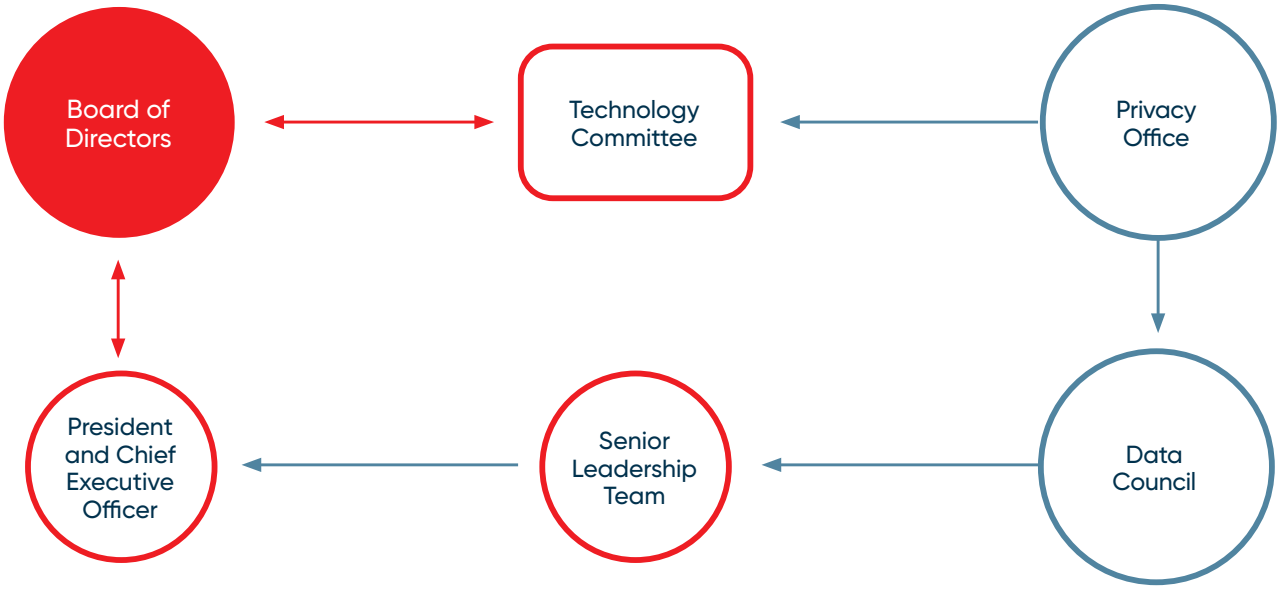
Our Commitment

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: to build and maintain a relationship 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 advances the United Nations (UN) Sustainable Development Goals, and goal 16 in particular: Peace, Justice and Strong Institutions. We have put in place a governance framework for the protection of personal information to ensure that we protect your information and maintain a relationship of trust with you.

Our Privacy Governance Framework



Privacy Office

The Privacy Office (the Office) is headed by the Chief Privacy Officer, who develops and implements our privacy program and privacy strategy and whose responsibilities include oversight related to:

- Developing, updating and implementing relevant documents in support of our privacy program, such as our policies, standards and procedures;
- The privacy risk governance framework; and
- Establishing appropriate controls for risk mitigation.

The Office's responsibilities include:

- Supporting the Bank's business sectors in carrying out the adopted strategic orientations;
- Ensuring compliance with best practices;
- Analyzing emerging issues that may affect our internal practices and our commitments to you; and
- Making recommendations to various decision-making levels.

The Privacy Office 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.

The Board of Directors and the Technology Committee

The Bank's **Board of Directors**, through the **Risk Management Committee and the Technology Subcommittee**, ensures that the Bank's technology strategy as well as its oversight and management of technology risks, including cyber risks, cybercrime and the protection of personal information, are properly applied and carried out.

The Data Council

The **Data Council** is composed of the Bank's executives and is interested in how the Bank manages data, including personal information, with a mandate to set the Bank's strategic orientations. At its monthly meetings, the Council is required to approve initiatives involving personal information that could have a significant impact on the orientations adopted by the Bank. The Data Council is supported by committees that assist in data risk oversight. For example, the **Data Risk Committee** oversees the integration of data risks, including privacy risks, into the risk management processes across various sectors.

The Executive Officers

The President and Chief Executive Officer as well as the Senior Leadership Team approve the main orientations and priorities regarding the strategy relating to the protection of personal information. They are ambassadors within the organization and to the Bank's Board of Directors with regard to the protection of personal information.

Strengthening our governance through privacy champions

As an institution, 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 Office on the ground.

The role of the privacy champion is to:

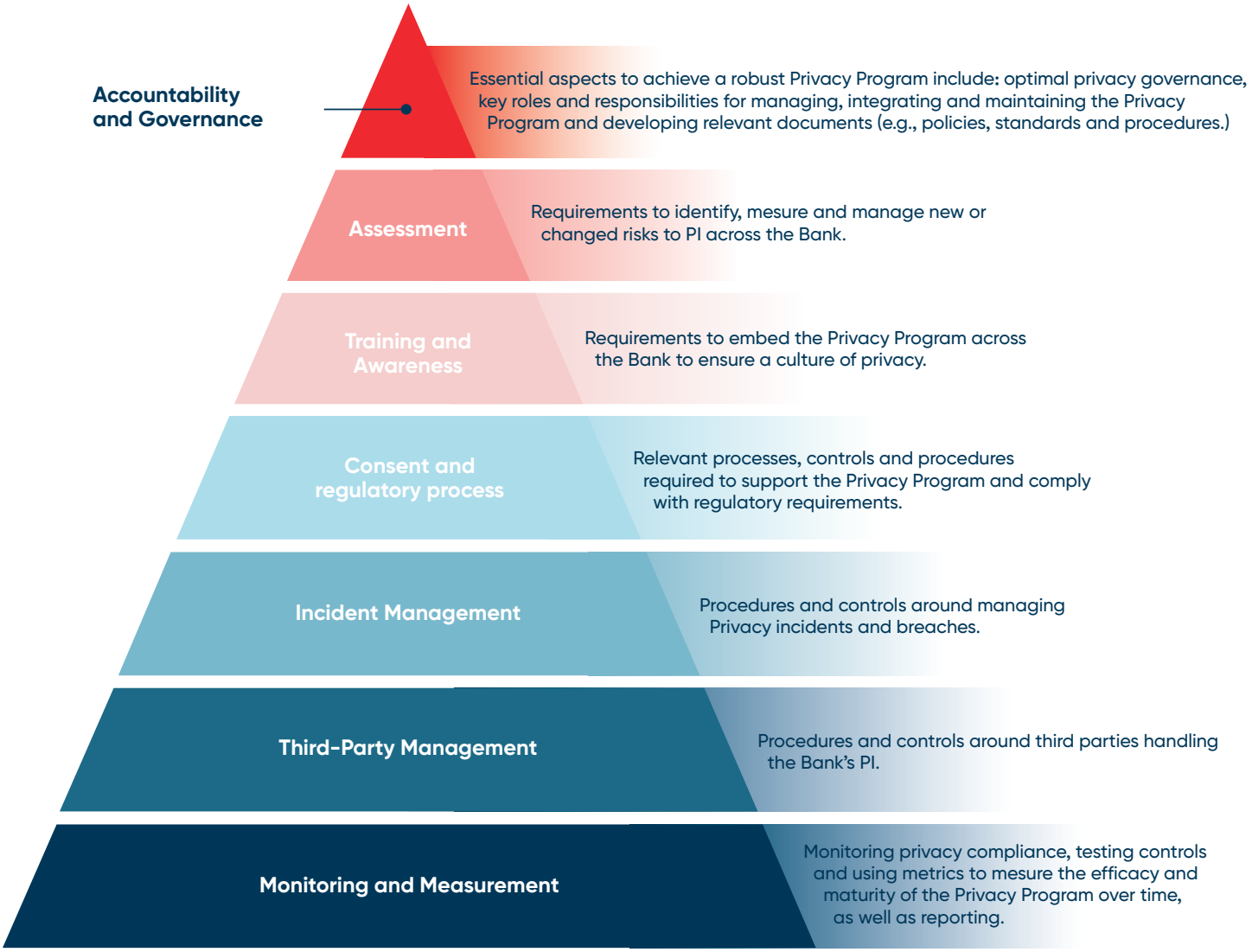
- Support business sectors with the development and implementation of projects, processes and control to ensure sound management of personal information;
- Identify business issues as well as any awareness and training needs for the business sectors they support;
- Support business sectors assess privacy-related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

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**. This process 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.

Our Privacy Program

The protection of individuals' personal information is crucial to accelerate our business model and strategies. Indeed, compliance with the various privacy requirements, as well as managing and safeguarding personal information appropriately are the basis of the relationship of trust with all our stakeholders. Proper management of personal information preserves and increases this relationship of trust, creates value for our clients and for our organization and reduces the risks associated with the processing of personal information. Our privacy program enables us to achieve these goals and it is based on the following seven pillars:



Our Privacy Practices

We oversee the protection of your personal information as follows:

- With a privacy policy, in which the Bank sets out the responsible practices it has adopted for the collection, use and disclosure of your personal information.
- Through effective **internal controls** to detect and prevent incidents throughout the entire life cycle of personal information.
- Through **continuous risk assessment: Several privacy related activities are in place to identify, assess and manage risks**, whether they are new or created as a result of technological changes, procedures or business initiatives.
- Through **complaint and incident management**.
- By providing **training** to all our employees.

Privacy Policy

We have developed our privacy policy with you in mind. **Your consent is the cornerstone of our practices:** we respect your choices and act based on the consent you have given.

This policy explains, among other things:

- What types of personal information we may collect and from whom;
- 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 retaining and destroying your personal information.

The policy also informs you about your rights to:

- Access and consult the personal information we have about you;
- Correct your personal information to ensure its accuracy;
- Opt out of receiving our product and service offers and other promotional communications at any time.

We will notify you of any significant changes to our policy when you enrol in new products or services through our digital channels and telephone banking services or via any other appropriate means we may use to communicate with you.

Ethical practices

Technological transformations, especially those related to artificial intelligence (AI) and advanced analytics technologies, are drawing more and more 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 program that focuses on fairness by design enables us to strengthen our AI and advanced analytics activities. This cross-sector program provides for concrete measures that help reinforce equity best practices and awareness and training activities for business development teams and data science teams alike. 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. In 2022, this adoption rate was 100%, with a target of 90%.

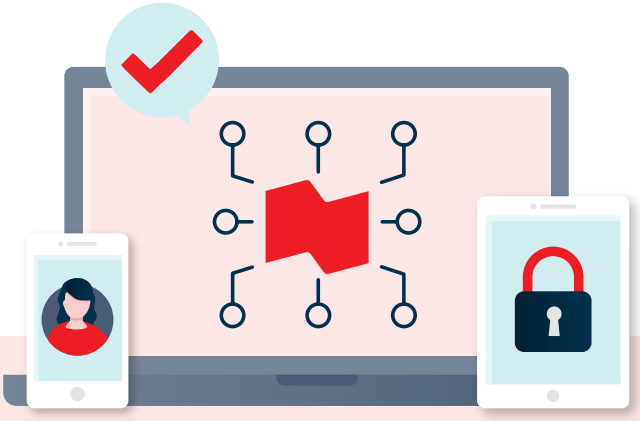
> Under no circumstances do we sell or provide customer lists to third parties for marketing purposes.

Training and awareness

Our approach is as follows:

1. Mandatory training for new hires that makes new employees aware of the importance of privacy for the Bank and our clients, and equips new employees with the tools to protect this information.
2. Continuously raising awareness through training modules and activities to keep employees informed.
3. Targeted training to support certain business sectors, for example, when deploying a new initiative or improving processes.

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



Annual Mandatory Training: Committed to Preserving Trust

In 2022, we deployed a new mandatory training on our commitment to maintaining a relationship of trust with our clients regarding the sound and responsible use of personal information.

91 % of active employees successfully completed the training.

In 2021, the training regarding privacy best practices was successfully completed by 92% of active employees

Consent of individuals training

In order to support our clients in their choices while demonstrating the added value of the use of their personal information, our employees working directly with clients have received training on the choices offered to clients regarding the use of personal information.

Relationship with our service providers and business partners

The safety of your personal information is important when it must be sent to third parties. We take great care in choosing our business partners and service providers. We 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 in all stages of the life cycle of a service provider or business partner.

The life cycle of a service provider or a business partner

- **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 due diligence review.
- **Negociation of Agreements:** Our service providers or business partners may only use personal information in a responsible and ethical 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 oversight mechanisms are in place to monitor, amongst other things, compliance with security and privacy requirements.
- **Renewal, Expiry or Termination of Agreements**: If we decide not to renew the agreement with our service provider or business partner, the Bank and its service provider or business partner follow the relevant contractual clauses, in particular those relating to the retrieval and the destruction of personal information.

Complaint and incident management

Complaint management

We want to offer you a personalized client experience in line with your expectations. Your complaints and dissatisfactions are taken seriously. Complaints are handled confidentially.

Our branch advisors, our Client Experience Centre and Privacy Office work together to answer your questions about the protection of your personal information, to guide you and find solutions that are right for you.

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

You can contact us in the following ways:

- reach out to the customer service manager of your branch
- reach out to your investment advisor or representative
- by writing to us at confidentiality@nbc.ca
- by writing to our Chief Privacy Officer

To make a complaint, you must follow the procedures outlined in our complaint resolution brochure, available in branches and on our website at **nbc.ca**, under About us > Useful links > Complaint settlement online.

Confidentiality incident management that may involve personal information

We work with several teams to protect your personal information from loss, theft or any other breach in the protection of personal information. We have practices in place that allow us to identify and fully understand the risks, and rectify situations that put your personal information at risk.

We are also improving the internal controls that are already in place.

If a situation arises, we take the lead in notifying the relevant regulatory authorities as well as any affected clients. Our goal is to reduce and mitigate risks by offering you appropriate solutions based on the situation.

Cross-border data movements

If it is necessary to move data across borders as part of our activities, we make sure to comply with applicable laws and the best practices in this area. Risk assessments are carried out taking into consideration the various legal and regulatory requirements, the legal and socio-political context of the recipient countries, the volume and sensitivity of the information shared – all in order to ensure that a comparable degree of protection to the country of origin can be offered. Four principles must be followed before proceeding with a cross-border movement of data: necessity, knowledge, evaluation and governance.

Life cycle of personal information

Life cycle of personal information

- **Collection:** We limit the collection of your information to what is necessary to help us provide you with good service.
- **Use:** We use your information in accordance with our Privacy Policy.
- **Communication:** At all times, we are committed to limit the 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 for longer periods as required or authorized by law. If you cease to do business with us, we will retain your information for a reasonable period of time following the end of the business relationship to meet our legal obligations.
- **Destruction:** When your information is no longer needed, we use reasonable efforts to securely destroy it.

For more information about our practices, please see our privacy policy.

Our Performance in 2022

Our practices are evolving. 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 2022 **0**

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. **Chief Privacy Officer** at:
   confidentiality@nbc.ca
   or
   600 De La Gauchetière Street West, 4th Floor
   Montreal, Quebec, Canada H3B 4L2

NATIONAL BANK

31959-002 (2023/01)