

Cahier de protection des renseignements personnels 2025





Table des matières

3	Notre mission commune
4	À propos de ce cahier
5	Notre engagement
6	Notre programme de protection des renseignements personnels
7	Pilier 1 : Responsabilité et gouvernance
9	Pilier 2 : Évaluation
11	Pilier 3 : Formation et sensibilisation
12	Pilier 4 : Consentement et gestion responsable des renseignements personnels
14	Pilier 5 : Gestion des incidents
15	Pilier 6 : Gestion des tiers
16	Pilier 7 : Évaluation et surveillance
17	Notre performance 2025
17	Des questions ou des commentaires?

Notre mission commune

Nous existons pour
avoir un **impact positif**
dans la vie des gens.

En bâtissant **des relations**
à long terme avec notre
clientèle, nos équipes
et la communauté.

L'humain d'abord.

Pourquoi une mission commune?

Notre mission commune s'inscrit dans la continuité de nos efforts pour demeurer un moteur du développement économique et social prépondérant. Elle est la réponse à un besoin collectif de faire évoluer les habitudes bancaires vers une mission humaine qui nous permettra d'atteindre nos objectifs et de mieux collaborer avec l'ensemble de nos parties prenantes.

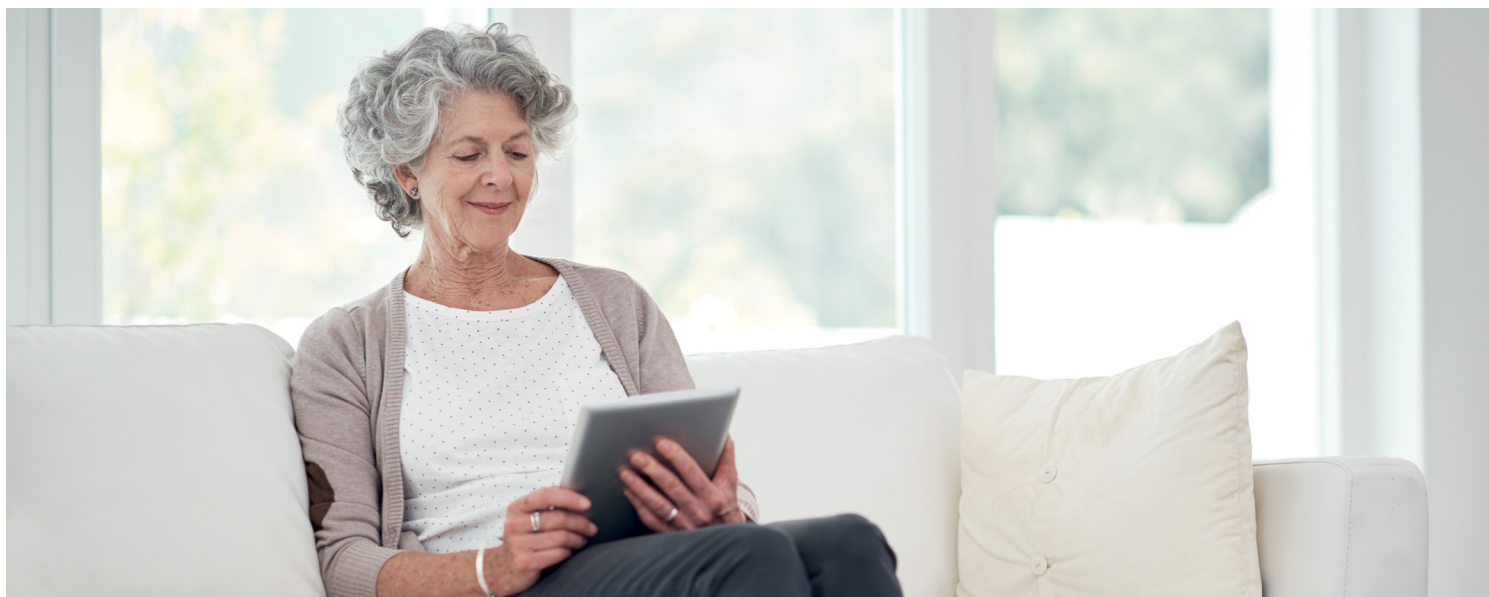
Comment se traduit concrètement notre mission commune?

- Par les expériences que nous voulons faire vivre à notre clientèle, à nos employé·e·s et à la communauté.
- Par nos comportements qui reflètent nos valeurs: complicité, pouvoir d'agir et agilité.
- Par la manière dont les employé·e·s travaillent ensemble afin d'augmenter la satisfaction de notre clientèle, l'engagement des employé·e·s et notre implication dans la communauté.
- Par les initiatives que nous priorisons pour avoir un impact positif.

À propos de ce cahier

Ce cahier consacré au thème de la **protection des renseignements personnels** est produit par l'équipe de la protection des renseignements personnels et de l'intelligence artificielle responsable de la Banque Nationale (Équipe). Il démontre notre volonté d'avancer avec vous en toute transparence et d'utiliser vos renseignements personnels de façon responsable. Ce cahier aborde également le rôle de l'Équipe dans l'élaboration de notre programme pour encadrer l'utilisation responsable de l'intelligence artificielle.

La protection des renseignements personnels fait partie des priorités de la Banque. Au fil des années, des mesures ont été mises en place afin de renforcer nos pratiques et d'assurer votre confiance. Nous vous les présentons dans ce cahier. Nous veillerons par la suite à vous présenter nos progrès et nos résultats annuellement.



Portée

Les informations contenues dans ce cahier couvrent les activités de la Banque et de ses principales filiales canadiennes⁽¹⁾ pour la période du 1^{er} novembre 2024 au 31 octobre 2025.

À qui il s'adresse – parties prenantes

Ce cahier a été préparé pour aider nos parties prenantes à comprendre notre programme de protection des renseignements personnels. Il reflète nos pratiques, nos politiques et nos normes en matière de protection des renseignements personnels et nos efforts de divulgation volontaire. Il vise également à susciter un dialogue en continu entre la Banque (y compris ses administrateur·trice·s et ses dirigeant·e·s) et sa clientèle, ses employé·e·s, ses actionnaires, ses fournisseurs ainsi que les communautés, les groupes d'intérêt et les autorités réglementaires. Ce dialogue nous permet d'enrichir nos pratiques et de viser les normes les plus avancées en matière de protection des renseignements personnels et de divulgation.

(1) Les informations présentées dans ce rapport n'incluent pas Technologies Flinks inc.

Notre engagement

Nous mettons tout en œuvre pour assurer la protection de vos renseignements personnels.

Tous nos employé-e-s collaborent à cet objectif.

Notre engagement envers vous est simple : faire et avancer ensemble, en toute confiance.

Cet engagement est aligné avec le volet Gouvernance de nos principes environnementaux, sociaux et de gouvernance (ESG), approuvés par le conseil d'administration de la Banque. Il contribue ainsi à faire avancer les objectifs de développement durable de l'Organisation des Nations Unies, notamment l'objectif 16 « Paix, justice et institutions efficaces ». En effet, nous avons mis en place un cadre de gouvernance pour la protection des renseignements personnels, afin de nous assurer de protéger vos renseignements et de maintenir une relation de confiance avec vous.

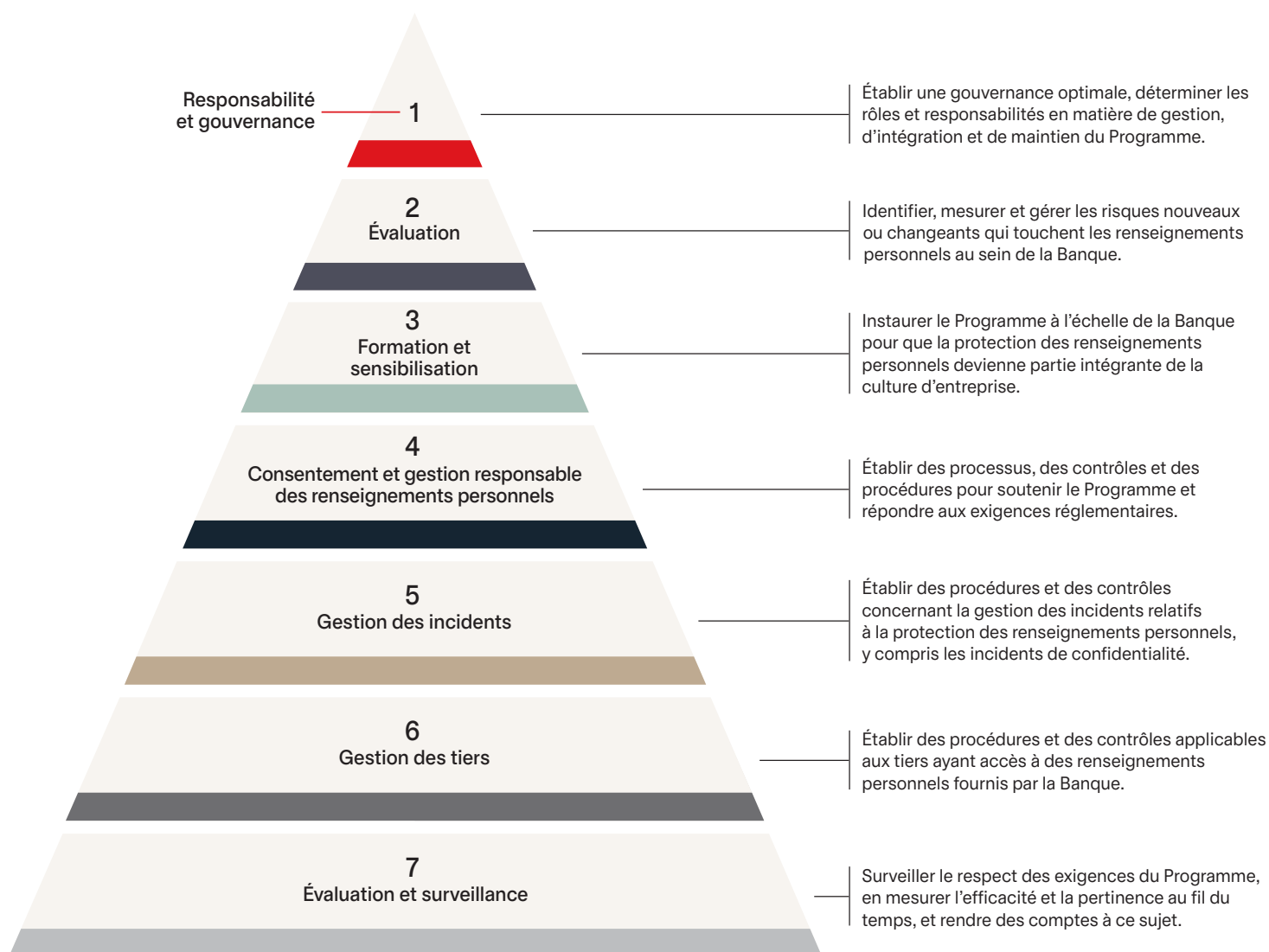
Faire et avancer ensemble, en toute confiance

→ Une utilisation
RESPONSABLE
de vos renseignements
personnels

→ Des mesures
SÉCURITAIRES pour
protéger vos renseignements
personnels

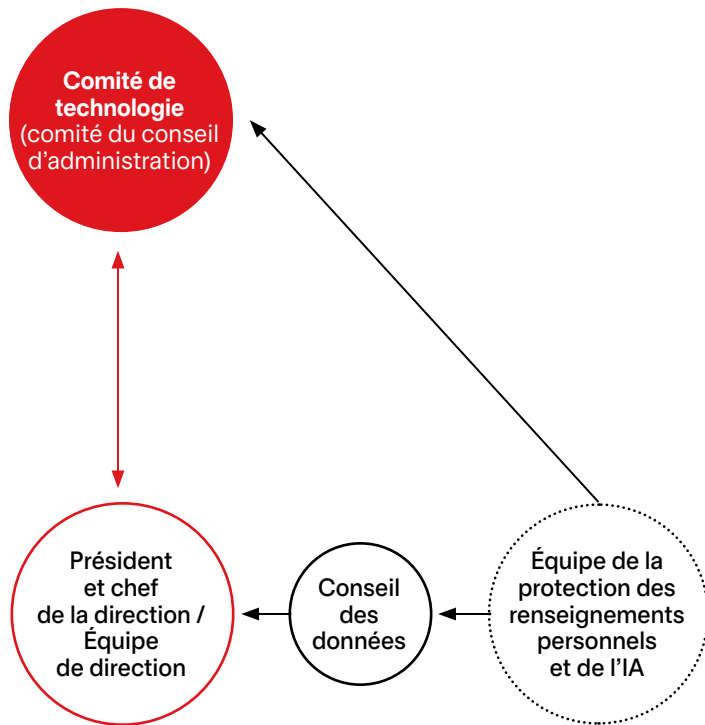
Notre programme de protection des renseignements personnels

La protection des renseignements personnels est essentielle pour accélérer nos stratégies d'affaires. Une saine gestion des renseignements personnels préserve et accroît la relation de confiance avec nos parties prenantes, crée de la valeur pour notre clientèle et pour notre organisation, et réduit les risques liés au traitement des renseignements personnels. Notre programme de protection des renseignements personnels nous permet d'atteindre ces objectifs et il s'appuie sur les sept piliers suivants :



Pilier 1 : Responsabilité et gouvernance

Nous avons adopté un cadre de gouvernance robuste qui définit les rôles et responsabilités de nos différentes équipes pour assurer la gestion, l'intégration et le maintien de notre programme de protection des renseignements personnels à travers l'organisation.



L'Équipe de la protection des renseignements personnels et de l'intelligence artificielle responsable (Équipe)

L'Équipe est dirigée par le chef de la protection des renseignements personnels et de l'intelligence artificielle (IA) responsable, qui relève du premier vice-président à la direction, Affaires juridiques, Technologie d'entreprise et résilience.

L'Équipe élabore et met en œuvre notre programme et notre stratégie liés à la protection des renseignements personnels. Elle est responsable :

- de l'élaboration, la mise à jour et la mise en œuvre des documents pertinents à l'appui de notre programme de protection des renseignements personnels;
- du cadre de gouvernance des risques liés à la protection des renseignements personnels;
- de recommander la mise en place de contrôles appropriés pour la mitigation des risques.

Le rôle de l'Équipe est, entre autres :

- d'assurer la protection et le traitement responsable des renseignements personnels ainsi que le respect des lois applicables;
- d'appuyer les secteurs d'affaires de la Banque dans l'exécution des orientations stratégiques adoptées;
- de surveiller de manière proactive toute nouvelle exigence législative en matière de protection des renseignements personnels et d'IA responsable et de veiller au respect des meilleures pratiques;
- d'examiner les enjeux émergents pouvant affecter nos façons de faire ainsi que nos engagements envers vous;
- d'émettre des recommandations aux différents paliers décisionnels;
- de participer à la socialisation de diverses initiatives de réforme de la protection des renseignements personnels et de l'IA responsable.

Elle présente périodiquement aux divers comités :

- des rapports sur les risques liés à la protection des renseignements personnels;
- des rapports sur les statuts d'avancement des initiatives stratégiques;
- les faits nouveaux ainsi que les tendances émergentes susceptibles d'avoir un impact sur les pratiques en place.

De plus, l'Équipe participe à l'élaboration et la mise en œuvre du programme d'IA responsable. Ainsi, elle collabore à :

- l'élaboration des politiques, normes et procédures encadrant l'utilisation responsable de l'IA;
- l'évaluation des risques liés à l'IA par la mise en place de processus d'évaluations multidisciplinaires;
- la création d'une équipe multidisciplinaire pour appuyer et accompagner les initiatives impliquant de l'IA;
- la création d'un cadre d'imputabilité au sein du cycle de vie des systèmes d'IA;
- l'intégration des huit principes de l'IA responsable dans les processus de conception, de développement et de déploiement des systèmes d'IA : responsabilité, proportionnalité, équité, sécurité, fiabilité, explicabilité, transparence et protection des renseignements personnels;
- l'élaboration d'un programme de formation destiné à l'ensemble des employé-e-s sur les bonnes pratiques en matière d'IA responsable.

Pilier 1 : Responsabilité et gouvernance (suite)

Le conseil d'administration et le comité de technologie

Le comité de technologie surveille les différentes composantes du programme de technologie de la Banque. Il examine, entre autres, la stratégie technologique de la Banque et supervise les risques technologiques, notamment en ce qui a trait aux cyberrisques, à la cybercriminalité, à la protection des renseignements personnels et à l'utilisation de l'IA. Le mandat et les principales réalisations du conseil d'administration et du comité de technologie peuvent être consultés dans les sous-sections du site Internet bnc.ca consacrées à la gouvernance et aux investisseurs, sous l'onglet « À propos de nous ».

Le conseil des données

Le conseil des données est composé de hauts dirigeants de la Banque. Il a pour mandat de veiller à maximiser la valeur d'affaires de la donnée, un actif important de la Banque. Il a le pouvoir de prendre des décisions concernant la façon dont la Banque gouverne, gère et exploite les données d'affaires sous sa responsabilité (y compris les renseignements personnels), en s'assurant du respect des politiques, normes ou pratiques les régissant et découlant du cadre d'appétit de la Banque.

La haute direction

Le président et chef de la direction ainsi que l'équipe de direction entérinent les grandes orientations et les priorités concernant la stratégie relative à la protection des renseignements personnels. Ils sont des ambassadeur·rice·s au sein de l'organisation et auprès du conseil d'administration de la Banque en matière de protection des renseignements personnels.

Renforcer notre gouvernance grâce aux partenaires de protection des renseignements personnels

Nous sommes engagé·e·s envers la création d'une culture soucieuse de la protection de vos renseignements personnels qui résonne au sein de toutes les fonctions de l'organisation. Afin de renforcer notre gouvernance, nous avons nommé des « Partenaires PRP » qui accompagnent différents secteurs d'affaires dans leurs initiatives afin d'utiliser le levier de la protection des renseignements personnels dans les stratégies d'affaires. Ils sont, en quelque sorte, les yeux et les oreilles de l'Équipe de la protection des renseignements personnels sur le terrain.

Le rôle d'un Partenaire PRP est principalement :

- de soutenir les secteurs d'affaires dans l'élaboration et la mise en place de projets et de processus destinés à assurer une saine gestion des renseignements personnels;
- d'identifier les enjeux d'affaires, les besoins de sensibilisation et de formations spécifiques aux secteurs d'affaires qu'ils accompagnent;
- d'accompagner les secteurs d'affaires dans l'évaluation des risques liés à la protection des renseignements personnels.

Nous travaillons à faire évoluer le rôle des Partenaires PRP afin qu'ils puissent soutenir les secteurs d'affaires dans leur utilisation responsable de l'intelligence artificielle et ainsi renforcer notre gouvernance dans ce domaine.

La protection des renseignements personnels, une responsabilité commune

La protection des renseignements personnels est le résultat d'une collaboration et d'efforts combinés de plusieurs secteurs d'affaires et comités internes. Notre gouvernance des renseignements personnels s'accompagne d'un **processus de reddition de compte**. Ce processus nous permet de mesurer l'efficacité de nos pratiques et de prendre des décisions basées sur notre engagement envers vous, notre appétit pour le risque ainsi que notre ambition de vous offrir des produits et solutions innovantes.

Pilier 2 : Évaluation

À la Banque, nous avons mis en place des processus pour identifier, évaluer et gérer les risques liés à la protection des renseignements personnels, qu'ils soient nouveaux ou évolutifs. Nos équipes opérationnelles se tiennent informées des enjeux entourant les renseignements personnels dans leurs domaines respectifs. Elles sont également responsables de cibler, évaluer et traiter les questions liées à la protection des renseignements personnels.

Évaluation des risques en continu

L'Équipe de la protection des renseignements personnels et de l'intelligence artificielle responsable supervise en continu plusieurs évaluations de risques portant sur la protection des renseignements personnels, dont celles concernant :

- les opérations de chaque secteur de la Banque;
- le traitement des plaintes liées à la protection des renseignements personnels;
- le traitement des incidents de confidentialité;
- l'intégration des tiers et fournisseurs.

L'Équipe veille ainsi à ce que les risques liés à la protection des renseignements personnels soient identifiés, évalués et gérés de façon constante au sein de l'organisation.



Évaluation des facteurs relatifs à la protection des renseignements personnels dès la conception

La Banque a élaboré un processus rigoureux qui lui permet d'évaluer les facteurs relatifs à la protection des renseignements personnels dès la conception de ses nouvelles initiatives ou de leur mise à jour. Ce processus vise à garantir une compréhension claire des risques liés à la protection des renseignements personnels associés à une initiative et à les atténuer. Le processus est complété par les équipes opérationnelles, en collaboration avec les Partenaires PRP et l'Équipe de la protection des renseignements personnels et de l'intelligence artificielle responsable.

Ce processus comporte trois étapes :

- 1** Une évaluation préliminaire de l'initiative pour déterminer son niveau de risque par rapport à la protection des renseignements personnels qui déclenche l'étape 2, si requis.
- 2** Une évaluation approfondie des répercussions de l'initiative sur la protection des renseignements personnels et l'identification des contrôles pour en atténuer les risques.
- 3** La mise en œuvre des contrôles identifiés.

Notre Équipe s'assure que le respect de votre vie privée demeure au centre de nos priorités dès la conception des initiatives.

Pilier 2 : Évaluation (suite)

Évaluation des mouvements transfrontaliers de données

S'il est nécessaire d'effectuer des mouvements transfrontaliers de données dans le cadre de nos activités, nous nous assurons de respecter les lois applicables et les meilleures pratiques. Un cadre strict sur les mouvements transfrontaliers de données est en place, qui inclut notamment :

- des évaluations des facteurs relatifs à la vie privée et des analyses de risques prenant en considération le volume, la sensibilité et l'utilisation envisagée des informations partagées; et
- des évaluations des pays destinataires prenant en considération le régime juridique applicable et le contexte légal et sociopolitique.

Ces diverses évaluations sont notamment effectuées afin de s'assurer qu'un degré de protection adéquat et comparable au pays d'origine peut être offert. Lorsqu'un tiers est impliqué, les processus d'évaluation des risques liés aux tiers sont appliqués, ce qui inclut des vérifications diligentes adéquates et la signature d'ententes contractuelles robustes.

Évaluation des facteurs relatifs à l'équité

Les transformations technologiques, spécialement celles liées aux technologies d'intelligence artificielle et d'analytique avancée, suscitent de plus en plus d'attention. Comme organisation, nous sommes conscients des effets que ces technologies peuvent avoir sur les droits et libertés ainsi que sur notre capacité de transformer positivement l'expérience de notre clientèle et de nos employé-e-s.

Pour ce faire, nous évaluons de manière proactive nos pratiques afin de veiller à ce que les technologies que nous déployons soient cohérentes avec nos valeurs.

À titre d'exemple, notre programme « d'équité dès la conception » (*fairness by design*) permet de renforcer nos activités en matière d'intelligence artificielle et d'analytique avancée responsables dès la conception des initiatives.

Ce programme inclut des mesures concrètes qui contribuent à solidifier les bonnes pratiques en matière d'équité. Dans ce contexte, des activités de sensibilisation et de formation ont été données au sein des différents secteurs de la Banque, tant aux équipes de développement des affaires que scientifiques ainsi qu'aux employé-e-s de la deuxième et troisième ligne de défense. Des indicateurs de performance sont en place pour assurer un suivi de nos pratiques sur l'équité. Par exemple, chaque année, nous suivons le taux d'adoption effectif du programme par les solutions analytiques que nous avons mises en production au cours de la dernière année.

Pilier 3 : Formation et sensibilisation

Notre approche est la suivante :

1. Une formation obligatoire à l'embauche qui sensibilise tout-e nouvel-le employé-e à l'importance de la protection des renseignements personnels pour la Banque et pour notre clientèle, et qui les outille en ce sens.
2. Une formation obligatoire annuelle sur la protection des renseignements personnels, dont le thème change chaque année pour bonifier les connaissances des employé-e-s dans ce domaine.
3. De la sensibilisation en continu par le biais de capsules et d'activités, afin de tenir les employé-e-s informé-e-s.
4. Des formations ciblées pour appuyer certains secteurs d'affaires, par exemple lors du déploiement d'une nouvelle initiative ou d'une amélioration de processus.

Notre objectif est d'avoir des employé-e-s mobilisé-e-s et sensibilisé-e-s à l'importance de la protection de vos renseignements personnels. La formation est offerte à tous les niveaux de notre organisation.

Les formations sont mises à jour périodiquement pour répondre aux nouvelles exigences réglementaires et aux meilleures pratiques. Notre Code de conduite renforce également l'importance de la protection des renseignements personnels.



Formation obligatoire à l'embauche : l'engagement BNC dans la protection des renseignements personnels

En 2025, cette formation a été suivie avec succès par les employé-e-s nouvellement embauché-e-s. Le taux de complétion des formations obligatoires à l'embauche dépasse les 99 % annuellement.

Formation obligatoire annuelle en 2025 : Adopter les comportements appropriés en protection des renseignements personnels

95 % des employé-e-s actif-ive-s lors du déploiement de la formation l'ont suivie.

De plus, la formation annuelle en sécurité a abordé le thème des bris de confidentialité, mettant en lumière les risques et les mesures préventives à adopter afin de réagir à ce type de bris.

Aussi, une formation sur l'utilisation de l'intelligence artificielle générative a été suivie par 97 % des employé-e-s actif-ive-s et soulignait l'importance d'une saine utilisation des renseignements personnels dans ce contexte.

Enfin, l'Équipe de la protection des renseignements et de l'intelligence artificielle responsable a publié sur les réseaux sociaux internes de la Banque de courtes capsules informatives sur des sujets d'intérêts reliés à la confidentialité et à la protection de la vie privée.

Pilier 4 : Consentement et gestion responsable des renseignements personnels

Nous élaborons et déployons des processus fiables pour traiter vos renseignements personnels de façon responsable conformément à vos attentes et aux lois applicables.

Comment nous respectons vos droits tout au long du cycle de vie de vos renseignements personnels

Collecte



Utilisation



Communication



Conservation



Destruction



- **La collecte** : Nous limitons la collecte de vos renseignements à ce qui est nécessaire pour nous aider à bien vous servir.
- **L'utilisation** : Nous utilisons vos renseignements conformément à notre Politique de protection des renseignements personnels et notre Politique sur les données numériques.
- **La communication** : En tout temps, nous nous engageons à limiter la communication de vos renseignements au strict nécessaire.
- **La conservation** : Nous conservons vos renseignements personnels aussi longtemps que nécessaire pour atteindre les fins auxquelles ils ont été recueillis ou aussi longtemps que requis ou permis par la loi. Pour déterminer les périodes de conservation de vos renseignements, nous avons pris en compte nos obligations légales, le but de la collecte ainsi que la nature et la sensibilité de vos renseignements. Nous avons révisé et simplifié nos délais de conservation pour clarifier l'événement déclencheur de la période de rétention.
- **La destruction** : Lorsque vos renseignements ne sont plus nécessaires, nous nous efforçons de les détruire en toute sécurité.

La documentation que nous mettons à votre disposition

Dans un esprit de transparence, nous avons publié deux politiques qui décrivent nos pratiques liées au traitement et à la protection de vos renseignements personnels :

- [La Politique de protection des renseignements personnels](#)
- [La Politique sur les données numériques](#)

Nous avons élaboré ces politiques en pensant à vous. En effet, votre consentement est la pierre angulaire de nos pratiques : nous respectons vos choix et agissons selon les consentements que vous donnez.

Pilier 4 : Consentement et gestion responsable des renseignements personnels (suite)

Politique de protection des renseignements personnels

Cette politique vous explique, entre autres :

- quels types de renseignements personnels nous recueillons et les raisons de la collecte;
- comment nous pouvons utiliser et communiquer les renseignements personnels et avec qui;
- le choix que vous avez de consentir ou non à certaines utilisations;
- notre approche en matière de protection et de conservation de vos renseignements personnels.

La politique vous informe aussi de vos droits :

- d'accéder aux renseignements personnels que nous détenons sur vous et d'en demander la communication;
- de corriger vos renseignements personnels pour en garantir l'exactitude;
- d'être informé-e lorsque nous prenons une décision exclusivement automatisée à votre sujet (sans intervention humaine), comme pour répondre à certaines demandes de crédit ou de financement;
- de refuser de recevoir nos offres de produits et services et autres communications de nature promotionnelle, en tout temps.

Politique sur les données numériques

Cette politique vous explique, entre autres :

- quels types de renseignements nous recueillons à l'aide de fichiers témoins et d'autres technologies similaires;
- les fins pour lesquelles nous recueillons ces renseignements;
- votre droit de refus et la façon de l'exercer ou de modifier vos préférences.

Vous avez des recours simples à votre disposition pour nous faire part de vos insatisfactions.

-
- Pour faire une plainte, vous devez suivre la procédure indiquée sur notre site Internet bnc.ca, sous **À propos de nous > Liens utiles > Résolution des insatisfactions**.
-

Gestion des demandes individuelles relatives aux renseignements personnels

De façon générale, lorsque vous formulez une demande pour avoir accès ou corriger vos renseignements personnels, nos employé-e-s y répondent dans les meilleurs délais après vous avoir authentifié-e. Si votre demande est complexe ou nécessite des recherches approfondies dans nos systèmes, elle est transférée à l'Équipe de la protection des renseignements personnels. Lorsque l'Équipe reçoit une telle demande, elle déploie les efforts nécessaires pour effectuer une recherche sérieuse et complète et y répondre à l'intérieur du délai de 30 jours suivant votre authentification. Si vous n'êtes pas satisfait-e de la réponse obtenue, vous disposez d'un recours devant le Commissariat à la protection de la vie privée du Canada, ou les régulateurs provinciaux en matière de protection des renseignements personnels, lorsqu'applicable.

Si vous préférez naviguer en ligne, notre solution automatisée vous permettra d'obtenir rapidement les renseignements personnels pertinents que nous détenons sur vous, ainsi que sur vos produits et services à la Banque Nationale. Pour ce faire, connectez-vous à votre banque en ligne, accédez à votre profil, choisissez l'onglet *Confidentialité*, choisissez ensuite *Faire une demande d'accès* et suivez les instructions. Vos renseignements seront déposés dans l'espace de partage de documents sécurisés, appelé *Ma voûte d'échange*, à l'intérieur de 30 jours.

Gestion des plaintes

La Banque veut être transparente quant à la façon dont elle gère vos renseignements personnels, en plus de s'assurer de les traiter de façon responsable. C'est pourquoi vos plaintes et vos insatisfactions relatives à la protection des renseignements personnels sont prises au sérieux. Afin de trouver rapidement des solutions qui vous conviennent, la Banque a élaboré et maintient son processus de traitement des plaintes relatives à la protection des renseignements personnels et forme ses employé-e-s pour les outiller dans la gestion de ce type de plaintes selon les procédures en place.

Nos employé-e-s et notre Équipe de la protection des renseignements personnels travaillent ensemble pour répondre à vos questions sur la protection de vos renseignements personnels, pour vous guider et trouver des solutions qui vous conviennent.

Pilier 5 : Gestion des incidents



Nous déployons des efforts importants afin de protéger vos renseignements personnels contre la perte, le vol, l'accès, l'utilisation ou la communication non autorisée. Nous avons des pratiques en place qui nous permettent de cibler et de bien comprendre nos risques. Nous avons élaboré un programme de sécurité pour suivre l'évolution constante des menaces à la sécurité des renseignements. Les mesures adoptées dans notre programme incluent :

- la protection de nos infrastructures, de nos locaux et de nos équipements;
- la gestion des accès à vos renseignements. Ainsi, seul-e-s les employé-e-s qui ont besoin de consulter vos renseignements dans le cadre de leurs fonctions y ont accès;
- la gestion des mots de passe et la mise en place des pare-feux;
- la vérification de sécurité à l'embauche de l'ensemble des employé-e-s de la Banque.

Si un incident devait survenir et présenter un risque sérieux, vous en seriez personnellement informé-e dans les délais prévus par la loi. De plus, la Banque s'assurerait d'informer les régulateurs pertinents ainsi que toute personne ou organisme susceptible de faire diminuer le risque de préjudice.

Pilier 6 : Gestion des tiers

Relation avec nos fournisseurs et partenaires d'affaires

La sécurité de vos renseignements personnels est importante, notamment lorsqu'ils doivent être transmis à des tiers. Nous choisissons avec soin nos partenaires d'affaires et nos fournisseurs de services. Nous avons un processus d'approvisionnement et de gestion des risques liés aux tiers. Lorsqu'il est nécessaire de faire appel à un fournisseur ou un partenaire d'affaires qui détiendra des informations (y compris des renseignements personnels) dont nous sommes responsables, notre processus est appliqué et les éléments liés à la protection des renseignements personnels sont intégrés dans toutes les étapes du cycle de vie d'un fournisseur de services ou d'un partenaire d'affaires.

Cycle de vie
d'un fournisseur
ou d'un partenaire
d'affaires

Évaluation



Vérification



Négociation
des contrats



Gestion
des contrats



Renouvellement
des contrats



→ En aucun cas, nous ne vendons des listes de client-e-s à des tiers.

- **L'évaluation de la matérialité** : Nous effectuons une évaluation de matérialité, laquelle comprend des questions relatives au risque lié à la protection des renseignements personnels.
- **La vérification diligente** : Nous procédons à une vérification diligente des éléments de sécurité et de protection des renseignements personnels.
- **La négociation des contrats** : Nos fournisseurs et nos partenaires d'affaires s'engagent à utiliser uniquement les renseignements personnels nécessaires à la prestation du service et à employer le même degré de diligence et de prudence que la Banque pour assurer la sécurité de vos renseignements personnels.
- **La gestion des contrats** : Nous nous assurons que les bons mécanismes sont en place pour surveiller, entre autres, le respect des exigences en matière de sécurité et de protection des renseignements personnels. Nous exigeons également de nous informer de tout incident de confidentialité afin que nous puissions travailler ensemble pour y répondre, y remédier et, le cas échéant, les signaler.
- **Le renouvellement, l'expiration ou la résiliation des contrats** : Si nous décidons de ne pas renouveler le contrat avec notre fournisseur de services ou notre partenaire d'affaires, la Banque et son fournisseur de services ou son partenaire d'affaires respectent les clauses contractuelles pertinentes, notamment celles concernant la récupération et la destruction des renseignements personnels.

Pilier 7 : Évaluation et surveillance

La Banque surveille son programme de protection des renseignements personnels en testant certains contrôles et en utilisant des mesures pour évaluer leur efficacité au fil du temps.

Chaque secteur d'affaires est responsable de surveiller l'efficacité des contrôles en place pour assurer la protection des renseignements personnels dans le cadre de ses opérations. Le secteur de la conformité effectue également une supervision indépendante de la conformité des pratiques de l'organisation aux exigences en matière de protection des renseignements personnels.

De plus, l'Équipe de la protection des renseignements personnels identifie et suit l'adoption des lois et règlements relatifs à la protection des renseignements personnels et s'assure de la mise en œuvre des nouvelles exigences au sein de l'organisation.



Notre performance 2025

Nos pratiques sont en pleine évolution. Nous enrichissons, en continu, nos indicateurs de performance afin de mesurer la qualité de nos pratiques. Le but est d'améliorer l'efficacité de nos stratégies et de nos processus opérationnels.

Nous avons mis en place un indicateur basé sur le nombre de décisions rendues annuellement par les organismes de réglementation visant la Banque.

Décisions en matière
de protection
des renseignements
personnels visant
la Banque



Objectif annuel visé
0



Résultat en 2025*
1

* La Commission d'accès à l'information du Québec a donné raison à la Banque dans un dossier de révision d'une demande d'accès aux renseignements personnels, confirmant ainsi qu'elle avait agi en conformité avec les lois applicables.

Des questions ou des commentaires?

Vos commentaires sont importants pour nous. Nous nous engageons à y donner suite de manière simple, afin de vous permettre de comprendre le traitement que nous accordons à vos renseignements personnels.

Pour tout commentaire ou question, vous pouvez communiquer avec :

1 Le directeur ou la directrice service
à la clientèle de votre succursale

2 Le chef de la protection des renseignements
personnels et de l'intelligence artificielle
responsable à l'adresse suivante :
confidentialite@bnc.ca
ou à la **Place Banque Nationale**
800, rue Saint-Jacques
Montréal (Québec) Canada H3C 1A3