Politique sur la gouvernance des données personnelles

**Avertissement et mise en contexte**

*Le Réseau de milieux naturels protégés tient à mentionner qu’après plusieurs lecture et recherche et étant donné que la loi 25 implique l’intégrité et la notoriété de votre organisation nous recommandons d’impliquer un avocat au terme ou en cours de rédaction d’une politique interne de gouvernance des données afin de s’assurer qu’elle est non seulement conforme aux lois et réglementations en vigueur, mais aussi qu’elle reflète les pratiques de l’organisme en matière de protection de la vie privée de ses utilisateurs. L’information contenue dans cette boite à outils est publiée de bonne foi afin d’aider les organismes membres du RMN à se conformer aux nouvelles exigences légales. Ces documents n’ont pas de valeurs officielles, et ne doivent pas être considérés comme étant exacts, opportuns ou destinés à un usage particulier. Le Réseau de milieux naturels ne garantit pas que l’information contenue dans ce document demeurera exacte, complète et à jour en tout temps. Toute utilisation de l’information contenue dans ce document doit être effectuée avec précaution et ne peut être interprétée comme constituant un avis juridique ou une opinion de quelque nature que ce soit. Dans toute la mesure permise en droit, Le Réseau de milieux naturels protégés ne sera en aucun cas responsable des dommages directs, indirects, exemplaires, accessoires ou particuliers, prévisibles ou non à l’égard de réclamation découlant de l’utilisation de l’information qui y est présentée.*

*Les documents de cette trousse à outils ont été développés grâce aux modèles mis à disposition par Bénévoles d’Expertise (« BE »). Vous pouvez retrouver les modèles originaux et d’autres informations pertinentes sur* [*leur site*](https://benevoles-expertise.com/loi-25/)*.*

# Introduction

La présente politique de gouvernance des données définit les principes et les pratiques qui guident la collecte, l'utilisation et la gestion des données personnelles par le Réseau de milieux naturels protégés. Elle comprend les normes et les directives techniques et comportementales pour la qualité, l’intégrité, la sécurité, la confidentialité, la conformité, la conservation et l’archivage des données personnelles, peu importe l’emplacement ou le format des données.

# Références et documents externes

* [Aide-Mémoire : Résumé des nouvelles dispositions de la Loi 25 visant à protéger la vie privée des Québécois](https://www.cai.gouv.qc.ca/documents/CAI_Guide_obligations_entreprises_vf.pdf)
* [Le site internet de la commission d’accès à l’information](https://www.cai.gouv.qc.ca/entreprises/)
* [La Loi fédérale sur la protection des renseignements personnels et les documents électroniques (LPRPDE)](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/r_o_p/)

# Définitions

* Gouvernance des données personnelles: Ensemble des politiques, des normes, des procédures et des rôles pour gérer les données personnelles de manière responsable et éthique.
* Données : Ensemble des données détenues et utilisées par l’organisation, incluant sans si limiter, les données personnelles et professionnelles.
* Données personnelles : renseignements personnels qui portent sur une personne physique et permettent de l’identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée. Cette définition exclut les données professionnelles.
* Données professionnelles : renseignements et coordonnées relatifs aux contacts d’affaires : employeur, fonction, coordonnées professionnelles (adresse courriel, adresse de l’entreprise, numéro de téléphone professionnel, etc.)

# Rôles et responsabilités

### Le conseil d’administration

Le conseil d’administration a la responsabilité de superviser la gouvernance des données et de s'assurer que l'organisation utilise les données de manière responsable, éthique et sécurisée.

**Responsabilités :**

#### Le conseil d'administration doit s'assurer que des politiques encadrant la gestion des données personnelles sont mises en place au sein de l’organisme et doit s’assurer que les ressources nécessaires sont allouées à leur mise en œuvre.

#### Évaluer les risques liés aux données personnelles : Le conseil d'administration doit comprendre les risques liés à la collecte, au stockage et à l'utilisation des données de l'organisation et s'assurer que des mesures adéquates sont mises en place pour les atténuer.

#### Surveiller la conformité réglementaire : Le conseil d'administration doit s'assurer que l'organisation est en conformité avec les lois et les règlements en matière de protection des données. Il doit également surveiller les développements réglementaires et s'assurer que l'organisation s'adapte en conséquence.

#### Assurer la transparence et la responsabilité : Le conseil d'administration doit s'assurer que les politiques de gouvernance des données personnelles de l'organisation sont clairement communiquées à tous les employés, parties prenantes et autres personnes concernées. Il doit également s'assurer que l'organisation est responsable de la gestion de ses données et est transparente dans ses activités liées aux données personnelles.

### Responsable de la gouvernance des données

Le responsable de la gouvernance des données est chargé de superviser et de garantir que l’organisme se conforme aux lois et réglementations applicables en matière de protection des données personnelles. Il est également responsable de sensibiliser les employés de l'organisation à l'importance de la protection des données et de mettre en place des politiques et des procédures pour assurer une saine gestion des données au sein de l’organisme.

Par défaut, le responsable de la gouvernance des données est la personne occupant la direction générale de l’organisation. Ce pouvoir peut être délégué par écrit à une personne disposant des compétences requises et un pouvoir décisionnel important.

**Responsabilités :**

#### Surveiller la conformité réglementaire de l'OBNL aux lois et réglementations applicables en matière de protection des données, notamment la Loi 25 du Québec qui vise la protection des renseignements personnels.

#### Élaborer des politiques et des procédures pour assurer la protection des données personnelles de l'organisation. Ces politiques et procédures peuvent inclure des politiques de confidentialité, des procédures de contrôle d'accès et des protocoles de gestion des incidents.

#### Évaluer les risques liés à la collecte, au stockage et à l'utilisation des données de l'organisation et mettre en place des mesures pour les atténuer.

#### S'assurer que les mesures de sécurité appropriées sont en place pour protéger les données contre les accès non autorisés, les pertes ou les altérations.

#### Sensibiliser le personnel de l'organisation à l'importance de la protection des données personnelles et leur fournir des formations régulières pour s'assurer que les employés comprennent leur rôle dans la protection de la vie privée des personnes concernées.

#### Gérer les demandes d'exercice de droits des personnes concernées, telles que le droit d'accès, de rectification ou de suppression de leurs données personnelles.

### Créateurs de données personnelles

Les créateurs de données sont responsables de la collecte de données en utilisant des méthodes valides et fiables. Ils doivent s'assurer que les données collectées sont pertinentes pour les objectifs de l'organisation.

Les responsables de la création de données sont les chargés de projets pour les projets où la collecte des données est nécessaire.

**Responsabilités :**

#### S’assurer du respect des normes de confidentialité en matière de données et garantir que les données sont stockées et gérées de manière sécurisée.

#### Documenter les données de manière complète et précise.

#### Respecter les politiques de l'OBNL en matière de données, en veillant à ce que les données soient utilisées de manière responsable et appropriée et en garantissant que les données sont partagées de manière responsable et conforme aux lois et règlements applicables.

### Utilisateur de données

Les utilisateurs doivent utiliser les données personnelles de manière responsable et appropriée, conformément aux lois et règlements applicables et aux politiques de l'OBNL en matière de données. Ils doivent également respecter les droits de confidentialité des personnes dont les données sont collectées.

**Responsabilités :**

#### Protéger les données contre l'accès non autorisé, la divulgation ou la perte en utilisant des mesures de sécurité appropriées.

#### Signaler tout problème lié aux données, y compris les violations de données ou les préoccupations de sécurité, au responsable de la gouvernance des données de l’organisme.

#### Respecter les politiques de l'OBNL en matière de données, en veillant à ce que les données soient utilisées de manière responsable et appropriée et en garantissant que les données sont partagées de manière responsable et conforme aux lois et règlements applicables.

# Directives

Cette section énonce les principes qui guident la gestion des données personnelles par le Réseau de milieux naturels protégés. Lors du développement de nouveaux projets ou de la collecte de nouvelles données, il est indispensable de s’y référer.

## Sécurité

L’utilisation personnelle des données du Réseau de milieux naturels protégés, y compris les données dérivées, dans n’importe quel format et à n’importe quel endroit, est interdite.

Les dossiers stockés dans un format électronique doivent être protégés par des mesures de protection électroniques appropriées et/ou des contrôles d’accès physique qui restreignent l’accès uniquement aux utilisateurs autorisés. De même, les données de l’entreprise (bases de données, etc.) doivent être stockées d’une manière qui limitera l’accès uniquement aux utilisateurs autorisés.

Par exemple, les données du Répertoire des sites de conservation volontaire doivent être accessibles aux seuls employés travaillant sur ce projet.

Cette politique s’applique aux documents de tous formats (papier, numérique ou audiovisuel), qu’ils soient des fichiers enregistrés, des documents de travail, des documents électroniques, des courriels, des transactions en ligne, des données conservées dans des bases de données, sur bande, sur disque, des cartes, des plans, des photographies, des enregistrements sonores et vidéos.

## Rétention des données personnelles

Toutes les données personnelles sont conservées conformément à nos obligations légales ou aussi longtemps que nécessaire pour parvenir aux fins pour lesquelles elles ont été recueillies et pour respecter les obligations légales de l’organisme. Le délai de rétention est calculé à partir de la date de la dernière mise à jour.

## Sauvegarde et restauration

La fréquence, l’étendue et la conservation des sauvegardes doivent être conformes à l’importance de l’information et au risque acceptable déterminé par le responsable de la gouvernance des données. Les activités de sauvegardes et de restauration des données doivent respecter les bonnes pratiques de gestion des données (Voir guide en [Annexe 1](#_Annexe_1)).

## Classification

La classification des données s'applique à toutes les données personnelles de l'organisation, quel que soit leur format (papier, électronique, etc.) ou leur emplacement (serveurs internes, services cloud, etc.). La classification des données se trouve dans le dictionnaire de données de l’organisme.

Le Réseau de milieux naturels protégés adopte les niveaux de classification de données suivants :

### Données confidentielles : Toute donnée qui, si elle était divulguée, pourrait causer un préjudice à l'organisme, à ses membres ou à ses parties prenantes. Les données confidentielles doivent être stockées dans des systèmes sécurisés et ne doivent être accessibles qu'aux personnes autorisées.

### Données internes : Informations accessibles aux employés et aux non-employés autorisés (administrateurs, bénévoles, consultants et sous-traitants) qui ont besoin de les connaître à des fins professionnelles.

### Données publiques : Toute donnée qui peut être librement partagée avec le public sans risque de préjudice pour l'organisation, ses membres ou ses parties prenantes. Les données publiques peuvent être diffusées librement.

## Dictionnaire de données personnelles

Le Réseau de milieux naturels protégés centralise l’ensemble des données personnelles de l’organisme dans le dictionnaire de données. Ce registre décrit toutes les données personnelles utilisées dans l'organisation, y compris leur définition, leur source, leur format, leur usage et leur classification.

## Accès aux données personnelles

Le Réseau de milieux naturels protégés protège ses actifs de données personnelles grâce à des mesures de sécurité qui assurent un accès approprié aux données lorsqu’elles sont consultées. Chaque élément de données personnelles est classifié et approuvé par le responsable de la gouvernance des données pour avoir un niveau d’accès approprié. L’accès aux données sera effectué conformément aux politiques de sécurité.

## Utilisation des données personnelles

Les administrateurs, employés, les contractuels et les bénévoles doivent accéder aux données personnelles et les utiliser uniquement dans la mesure requise pour l’exécution de leurs fonctions, et non à des fins personnelles ou à d’autres fins inappropriées. Ils doivent également accéder aux données et les utiliser selon les niveaux de sécurité attribués aux données. L’utilisation des données est classée dans les catégories suivantes : mise à jour, lecture seule et diffusion externe.

5.7.1 Mise à jour : l’autorisation de mettre à jour les données doit être accordée par le responsable de la gouvernance des données de l’organisme (ou une personne responsable désignée) aux personnes dont les tâches spécifient et exigent la responsabilité de la mise à jour des données.

5.7.2 Lecture seule : l’accès en lecture seule doit être autorisé par le responsable de la gouvernance des données de l’organisme (ou une personne responsable désignée) aux personnes dont les tâches nécessitent l’accès aux données.

5.7.3 Diffusion externe : Toute divulgation des données doit être approuvée par le responsable de la gouvernance des données de l’organisme (ou une personne responsable désignée) et doit être guidée par la nécessité de respecter la vie privée individuelle et de protéger l’intégrité des données.

## Application

Cette politique doit être respectée par tous les administrateurs, employés, contractuels et bénévoles du Réseau de milieux naturels protégés. La vérification de la conformité à cette politique est la responsabilité du responsable de la gouvernance des données de l’organisme. Les conséquences de la violation de cette politique dépendront des faits du cas, y compris la nature de la violation, l’existence de violations antérieures de cette politique ou d’autres politiques de l’organisme, la gravité de la violation et les lois applicables.

Approuvé par résolution XX

Date d’entrée en vigueur : XX septembre 2023

Annexe 1 – Guide des bonnes pratiques de sauvegarde et de restauration des données

Les bonnes pratiques de sauvegarde et de restauration des données peuvent varier en fonction des besoins et des contraintes de chaque organisation, mais voici quelques exemples généraux :

Informations numériques :

1. Effectuer des sauvegardes régulières : la fréquence des sauvegardes dépend du volume de données, de la fréquence de modification et de la criticité des données. Cependant, les sauvegardes doivent être effectuées régulièrement pour minimiser les pertes de données en cas de défaillance.

2. Utiliser des emplacements de sauvegarde hors site : pour garantir la sécurité des données, il est conseillé de stocker les sauvegardes sur un site différent du site principal. Cela peut aider à protéger les données contre les incendies, les inondations, les vols et d'autres incidents similaires.

3. Tester régulièrement les sauvegardes : les sauvegardes ne sont utiles que si elles peuvent être restaurées avec succès. Il est donc essentiel de tester régulièrement les sauvegardes pour s'assurer qu'elles peuvent être restaurées en cas de besoin.

4. Utiliser la méthode de sauvegarde appropriée : il existe plusieurs méthodes de sauvegarde, telles que la sauvegarde complète, la sauvegarde différentielle et la sauvegarde incrémentielle. Le choix de la méthode dépend de la quantité de données, de la fréquence des modifications et de la vitesse de sauvegarde et de restauration.

5. Utiliser des logiciels de sauvegarde fiables : Il est essentiel d'utiliser des logiciels de sauvegarde fiables pour garantir l'intégrité des données sauvegardées.

6. Mettre en place des politiques de sécurité pour les sauvegardes : les sauvegardes contiennent des informations sensibles, il est donc important de mettre en place des politiques de sécurité pour protéger les données contre les menaces internes et externes.

7. Établir une procédure de restauration documentée : il est essentiel d'établir une procédure de restauration documentée pour permettre une restauration rapide et efficace en cas de besoin.

8. Surveiller les sauvegardes : Il est important de surveiller les sauvegardes pour détecter les erreurs et les problèmes potentiels avant qu'ils ne deviennent des problèmes majeurs.

Documents physiques :

1. Utiliser un système de contrôle d'accès : Il est essentiel de mettre en place un système de contrôle d'accès pour empêcher l'accès non autorisé aux documents confidentiels. Les mesures de sécurité peuvent inclure l'utilisation de serrures, de codes d'accès et de caméras de surveillance.

2. Stocker les documents dans un endroit sécurisé : les documents confidentiels doivent être stockés dans un endroit sûr et sécurisé pour minimiser les risques de vol et de perte. Un lieu de stockage verrouillé et équipé d'un système d'alarme peut être un choix judicieux.

3. Limiter l'accès aux documents confidentiels : il est important de limiter l'accès aux documents confidentiels uniquement aux employés qui ont besoin d'y accéder. Des contrôles d'accès physiques et des politiques de sécurité strictes peuvent être nécessaires.

4. Protéger les documents pendant le transport : les documents confidentiels doivent être protégés pendant le transport pour éviter tout accès non autorisé ou tout vol. Des mesures de sécurité telles que le scellage des boîtes et des sacs de transport peuvent être mises en place.

5. Détruire les documents confidentiels de manière sécurisée : les documents confidentiels doivent être détruits de manière sécurisée pour éviter tout accès non autorisé aux informations sensibles. Des méthodes telles que la déchiqueteuse de papier et le broyage sont des options à considérer.

6. Former les employés sur les politiques de sécurité : il est important de former les employés sur les politiques de sécurité en place pour les documents confidentiels. Les employés doivent comprendre les mesures de sécurité en place et les risques associés à la divulgation d'informations sensibles.

Annexe 2 - FICHE D’INFORMATION SUR LA DESTRUCTION DES DOCUMENTS CONTENANT DES RENSEIGNEMENTS PERSONNELS

Tout organisme ou toute entreprise privée qui recueillent, détiennent, utilisent ou communiquent des renseignements personnels doivent mettre en place des mesures de sécurité propres à préserver le caractère confidentiel de ces données. Cette obligation découle à la fois de la Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé. À la suite d’incidents majeurs qui lui ont été signalés, la Commission d’accès à l’information a réfléchi sur les moyens à prendre pour assurer la protection du caractère confidentiel des renseignements personnels au moment de leur destruction.

Au sein de l’organisme ou de l’entreprise, il est important que chaque employé, à son poste de travail, se sente responsable d’assurer la protection des renseignements personnels qu’il traite. C’est ainsi qu’il ne doit pas jeter au rebut les documents, cartes de mémoire flash, clés USB, disques durs d’ordinateur, CD, DVD, etc. qui en contiennent, sans s’être assuré au préalable que leur contenu ne peut être reconstitué.

La Commission suggère aux organismes et entreprises de désigner une personne qui sera responsable de mettre en place et de surveiller l’application d’une politique sur la destruction de documents contenant des renseignements personnels.

Le déchiquetage de documents sur support papier, le formatage de médias numériques réutilisables et la destruction physique de médias numériques non réutilisables demeurent les meilleures méthodes de destruction des documents confidentiels. Si les spécifications techniques de la déchiqueteuse de l’entreprise ne répondent pas au volume des documents sur support papier à détruire, il faut les entreposer dans un endroit fermé à clé avant de les confier à une entreprise spécialisée de récupération de papier.

La Commission voit mal comment la destruction des documents contenant des renseignements personnels puisse s’effectuer sur la foi d’une simple entente verbale. Aussi, un contrat en bonne et due forme concernant la destruction des documents devrait-il contenir au moins des clauses spécifiant :

- le procédé utilisé pour la destruction des documents ;

- la nécessité d’un accord préalable entre les parties avant de confier la destruction des documents confidentiels à un sous-contractant ;

- les pénalités aux dépens de l’entreprise de récupération si elle ne respecte pas ses engagements.

En outre, dans ce même contrat, la Commission est d’avis que l’entreprise de récupération devrait :

- reconnaître que les renseignements personnels contenus dans les documents sont de nature confidentielle ;

- faire signer un engagement à la confidentialité à toute personne qui aura à manipuler ces documents ;

- s’engager à ce que les documents soient entreposés dans des locaux sécuritaires et qu’ils soient toujours sous bonne garde jusqu’à leur destruction ;

- veiller à limiter de façon très stricte l’accès aux lieux où les documents sont entreposés ou transformés ;

- s’engager à ne pas céder les documents en sa possession à des tiers à des fins autres que la transformation du papier préalablement et obligatoirement déchiqueté ;

- assurer à son client le droit d’avoir accès en tout temps à ses installations, toute la durée du contrat ;

- voir à la destruction totale des documents qui ne font pas l’objet d’une transformation ;

- faire rapport à son client lors de la destruction des documents reçus.