POLITIQUE DE CONFIDENTIALITÉ ET DE GESTION DES RENSEIGNEMENTS PERSONNELS

CBRCR
Conseil de bassin de la rivière du Cap Rouge

Adoptée par le conseil d'administration
Entrée en vigueur : 16 septembre 2024

1 Introduction

La présente Politique de confidentialité et de gestion des renseignements personnels (« Politique » définit les principes et les pratiques qui guident la collecte, l'utilisation et la gestion des renseignements personnels par *le Conseil de bassin de la rivière du Cap Rouge (« CBRCR » ou « l'organisme »)*. 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, peu importe l'emplacement ou le format des données.

Cette politique a pour objectif d'informer les utilisateurs des raisons et de la façon dont le CBRCR, ou toute personne agissant en son nom, collecte et utilise leurs renseignements personnels. Elle veut s'assurer d'un consentement éclairé des utilisateurs. Dans la mesure du possible, le CBRCR anonymise, pseudonymise et/ou agrége les renseignements personnels afin qu'ils n'identifient plus une personne.

2 Définitions

- Créateur de données: Toute personne, administrateur.trice ou employé.e du CBRCR, chargée de la collecte de certains renseignements personnels;
- Donnée: Toute information stockée, collectée, traitée ou utilisée, quel que soit le format ou le support utilisé;
- Gouvernance des données: Ensemble des politiques, des normes, des procédures et des rôles pour gérer les renseignements personnels de manière responsable et éthique;
- Incident de confidentialité : il s'agit des cas suivants :
  - l'accès non autorisé par la loi à un renseignement personnel;
  - l'utilisation non autorisée par la loi d'un renseignement personnel;
  - la communication non autorisée par la loi d'un renseignement personnel;
  - la perte d'un renseignement personnel ou tout autre atteinte à la protection d'un tel renseignement.

- Loi : *Loi sur la protection des renseignements personnels dans le secteur privé* (RLRQ chapitre P-39.1);
- Renseignements personnels : Une donnée visant une personne physique et qui permet de l'identifier directement ou indirectement, touchant entre autres l'une des catégories suivantes :
  - **Renseignements d'identification**
    Adresse, numéro de téléphone, sexe, âge, numéro d'assurance sociale, numéro d'assurance maladie, identifiant numérique, etc.
  - **Renseignements de santé**
    Dossier médical, diagnostic, consultation d'une professionnelle ou d'un professionnel de la santé, médicament, ordonnance, renseignements sur la cause d'un décès, etc.

▪**Renseignements financiers**
Revenu d'une personne, renseignements relatifs à l'impôt, numéro de compte bancaire, biens possédés, numéros de cartes de crédit, etc.
▪**Renseignements relatifs au travail**
Dossier disciplinaire, motifs d'absence, dates de vacances, salaire, évaluation du rendement, heures d'entrée et de sortie liées au lieu de travail, etc.
▪**Renseignements scolaires et relatifs à la formation**
Inscription à des cours, choix de cours, résultats scolaires, diplômes, curriculum vitæ, etc.
▪**Renseignements relatifs à la situation sociale ou familiale**
Documents qui attestent l'état civil, le fait qu'une personne ait ou non des enfants ou qu'elle reçoive des prestations d'aide sociale ou de chômage, etc.

Les renseignements personnels sont confidentiels, sauf dans les cas prévus par la loi. Ils doivent être protégés conformément à la Loi sur l'accès.

- Utilisateur de données : Toute personne, administrateur.trice ou employé.e du CBRCR, utilisant un renseignement personnel collecté par le CBRCR;

3 Rôles et responsabilités

3.1 Le conseil d'administration

Le conseil d'administration s'assure que le Responsable supervise la gouvernance des renseignements personnels et s'assure que l'organisme utilise ces données de manière responsable, éthique et sécurisée.

Responsabilités:

3.1.1 Le conseil d'administration doit s'assurer que des politiques ou des procédures encadrant la gestion des renseignements personnels sont mises en place au sein de l'organisme et doit s'assurer que les ressources nécessaires sont allouées à leur mise en œuvre.

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

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

3.2 Responsable de la protection des renseignements personnels

Le Responsable de la protection des renseignements personnels (le « Responsable ») est la personne ayant la plus haute autorité au sein de l'organisme, soit le président du CBRCR, tel qu'il appert des dispositions des Règlements généraux de l'organisme. Le Responsable est chargé de superviser et de garantir que l'organisme se conforme aux lois et réglementations applicables en matière de protection des renseignements personnels . Il est également responsable de sensibiliser les employés de l'organisme à l'importance de la protection de ces données et de mettre en place des politiques et des procédures pour assurer une saine gestion des renseignements personnels au sein de l'organisme.

Responsabilités :

3.2.1 Surveiller la conformité réglementaire du CBRCR aux lois et réglementations applicables en matière de protection des renseignements personnels, notamment la Loi, laquelle vise la protection des renseignements personnels.

3.2.2 Élaborer des politiques et des procédures pour assurer la protection des renseignements personnels de l'organisme. Ces politiques et procédures peuvent inclure des politiques de confidentialité, des procédures de contrôle d'accès et des protocoles de gestion des incidents.

3.2.3 Évaluer les risques liés à la collecte, au stockage et à l'utilisation des renseignements personnels de l'organisme et mettre en place des mesures pour les atténuer.

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

3.2.5 Sensibiliser le personnel de l'organisme à l'importance de la protection des renseignements personnels 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.

3.2.6 Gérer les demandes d'exercice de droits des personnes concernées, telles que le droit d'accès, de rectification ou de suppression de leurs renseignements personnels.

3.2.7 Mettre en place un comité sur la protection des renseignements personnels (« Comité ») et, le cas échéant, déléguer à un.e administrateur.trice ou un.e employé.e, en tant que membre du Comité, certaines tâches et responsabilités du Responsable notamment par celles décrites ci-dessus.

3.3 Créateurs de données

Les créateurs de données, identifiés par le Responsable selon leurs tâches, sont responsables de la collecte des renseignements personnels en utilisant des méthodes valides et fiables. Ils doivent s'assurer que les données collectées sont pertinentes pour les objectifs de l'organisation.

Le Responsable, en concertation avec le Comité, peut modifier un formulaire de consentement existant ou créer tout nouveau formulaire permettant de recueillir des renseignements personnels dans le cadre des activités du CBRCR.

Responsabilités :

3.3.1 Respecter les normes de confidentialité en matière de renseignements personnels et garantir que ces données sont stockées et gérées de manière sécurisée.

3.3.2 Documenter les données de manière complète et précise.

3.3.3 Respecter les politiques et procédures du CBRCR en matière de renseignements personnels, en veillant à ce que ces données soient utilisées de manière responsable et appropriée et en garantissant que celles-ci sont partagées de manière responsable et conforme aux lois et règlements applicables.

3.4 Utilisateur de données

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

Responsabilités

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

3.4.2 Signaler tout problème lié aux renseignements personnels, y compris les violations de ces données ou les préoccupations de sécurité, au Responsable de l'organisme.

3.4.3 Respecter les politiques du CBRCR en matière de renseignements personnels, en veillant à ce que ces données soient utilisées de manière responsable et appropriée et en garantissant que celles-ci sont partagées de manière responsable et conforme aux lois et règlements applicables.

4 Directives

Le Responsable, en concertation avec le Comité, établit des instructions détaillées sur la manière dont les renseignements personnels doivent être gérés, utilisés et protégés au sein de l'organisme. Les directives énoncent les principes et les procédures à suivre pour garantir que ces données sont utilisées de manière responsable, transparente et conforme aux normes juridiques et éthiques.

4.1 Sécurité

Le Responsable, en concertation avec le Comité, établit les mesures de sécurité nécessaires pour protéger les renseignements personnels de l'organisme contre les menaces internes et externes, telles que les piratages informatiques, les vols de données et les fuites d'informations.

L'utilisation personnelle des renseignements personnels détenus par le CBRCR, 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'organisme contenant des renseignements personnels (bases de données, etc.) doivent être stockées d'une manière qui limitera l'accès uniquement aux utilisateurs autorisés.

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 ou sur bande ou sur disque, des cartes, des plans, des photographies, des enregistrements sonores et vidéos.

4.2 Rétention des données

Le Responsable, en concertation avec le Comité, s'assure de la rétention et de la destruction des données contenant des renseignements personnels conformément à la Loi sur les archives (RLRQ A-21.1). Un calendrier de rétention et de destruction du CBRCR est établi, et révisé annuellement, par le Comité, selon les besoins de l'organisme, et conformément à la loi.

Exemple d'un calendrier de rétention (non liant)	
Type de données	**Période de rétention**
Grands livres	Permanent
Relevés bancaires	7 ans
Contrats et baux	7 ans
Procès-verbaux des réunions du CA	Permanent
Registre des membres	À déterminer
Dossiers des employés	À déterminer
Etc…	

4.3 Sauvegarde et restauration

Le Responsable, en concertation avec le Comité, établit les mesures permettant de garantir la disponibilité, l'intégrité et la sécurité des renseignements personnels, de se conformer aux exigences réglementaires, de réduire les risques de perte de ces données et d'optimiser les coûts et les ressources associés à la sauvegarde et à la restauration de telles données.

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. Les activités de sauvegardes et de restauration des renseignements personnels doivent respecter les bonnes pratiques de gestion des données.

4.4 Accès aux renseignements personnels

Le Responsable, en concertation avec le Comité, met en place des mesures permettant de garantir que les renseignements personnels détenus par l'organisme sont accédés de manière sécurisée et appropriée.

Le CBRCR protège ses actifs de données grâce à des mesures de sécurité qui assurent un accès approprié aux données lorsqu'elles sont consultées. Chaque élément de données contenant des renseignements personnels est approuvé par le Responsable pour avoir un niveau d'accès approprié.

4.5 Utilisation des renseignements personnels

Les administrateurs, employés, les contractuels et les bénévoles doivent accéder aux renseignements personnels détenus par l'organisme 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. L'utilisation de ces données est classée dans les catégories suivantes : mise à jour, lecture seule et diffusion externe.

4.5.1 Mise à jour : l'autorisation de mettre à jour les renseignements personnels doit être accordée par le Responsable (ou une personne responsable désignée) aux personnes dont les tâches spécifient et exigent la responsabilité de la mise à jour de ces données.

4.5.2 Lecture seule : l'accès en lecture seule doit être autorisé par le Responsable (ou une personne responsable désignée) aux personnes dont les tâches nécessitent l'accès aux renseignements personnels.

4.5.3 Diffusion externe : Toute divulgation des renseignements personnels doit être approuvée par le Responsable de la (ou une personne responsable désignée) et doit être guidée par la nécessité de respecter la vie privée individuelle et de protéger l'intégrité de ces données.

5 Incident de confidentialité

Un incident de confidentialité est traité selon les modalités décrites à l'Annexe 1.

Le Responsable, en concertation avec le Comité, peut, dans le respect de la Loi, compléter ou préciser des éléments de l'Annexe 1.

6 Application

Le Responsable, en concertation avec le Comité, met en place les mesures concrètes à prendre pour mettre en œuvre les dispositions de la Politique.

Cette politique doit être respectée par tous les administrateurs, employés, contractuels et bénévoles du CBRCR. La vérification de la conformité à cette politique est la responsabilité du Responsable . 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.

ANNEXE 1

ANNEXE 1 TRAITEMENT D'UN INCIDENT

FIGURE I : SCHÉMA SUR LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL

(Articles 63.8 à 63.11 de la Loi sur l'accès aux documents des organismes public et sur la protection des renseignements personnels (LAI))

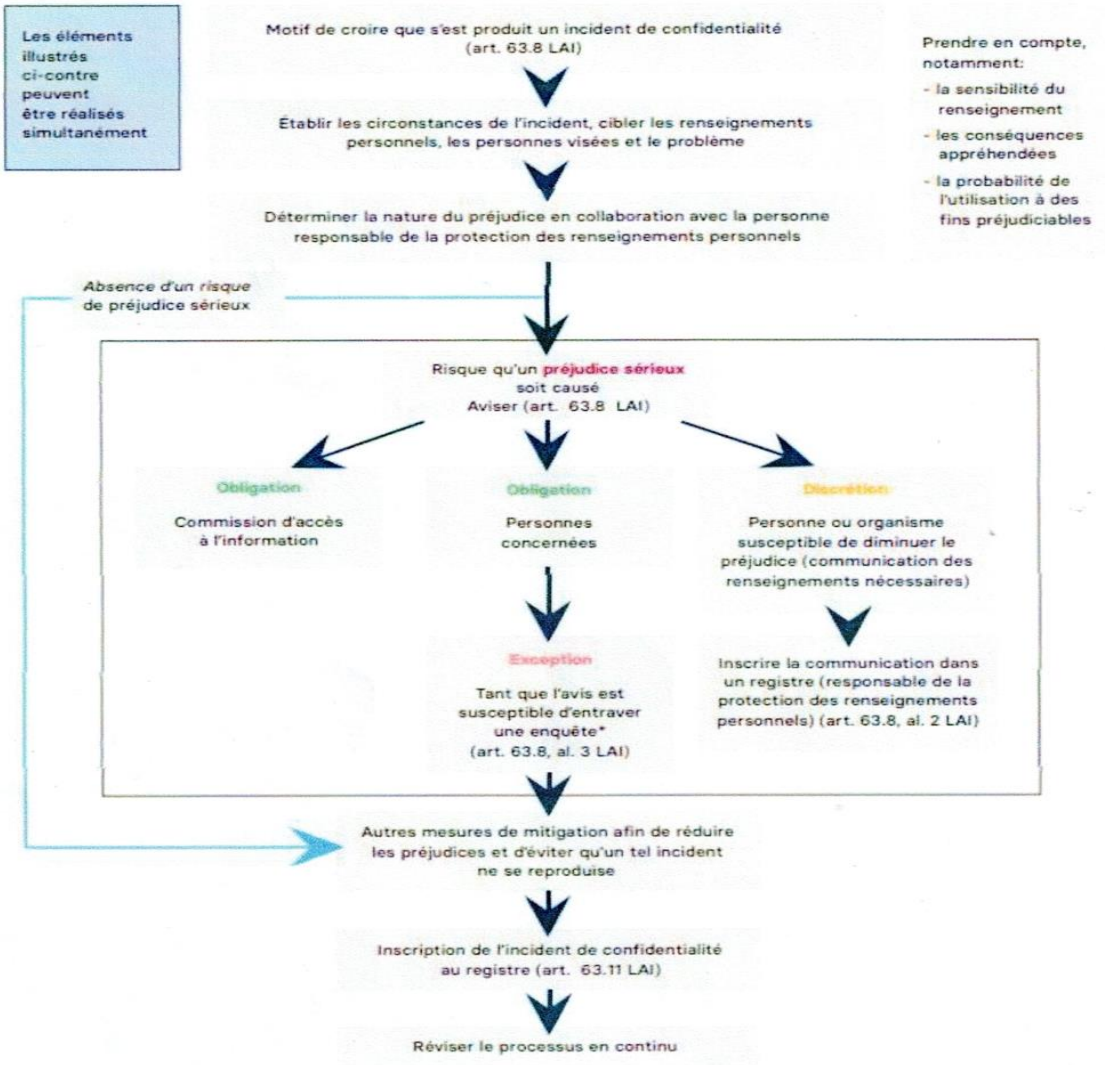

SCHÉMA SUR LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT UN RENSEIGNEMENT PERSONNEL
SOURCE : CONSEIL INTERPROFESSIONNEL DU QUÉBEC, 2022. LOI 25 - GUIDE D'ACCOMPAGNEMENT POUR LES ORDRES PROFESSIONNELS (CONSULTÉ LE 23 AOÛT. 2023)

7