FONDATION DUFRESNE & GAUTHIER

Politique interne de gouvernance des données

1 Introduction

La présente politique de gouvernance des données (ci-après la « Politique ») définit les principes et les pratiques qui guident la collecte, l'utilisation et la gestion des données par la *Fondation Dufresne & Gauthier* (ci-après la « Fondation »). 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.

2 Références et documents externes

- Politique sur la protection des renseignements personnels
- Aide-Mémoire : Résumé des nouvelles dispositions de la Loi 25 visant à protéger la vie privée des Québécois
- Le site internet de la commission d'accès à l'information
- La Loi fédérale sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

3 Champ d'application

La Politique s'adresse à tout le personnel de la Fondation, y compris les stagiaires et les membres du conseil d'administration.

Elle s'applique à tous les renseignements détenus par la Fondation, y compris ceux dont la conservation est assurée par un tiers, quel que soit le support sur lequel ils sont conservés, et ce, de leur collecte à leur destruction. Tout renseignement qui concerne une personne physique et qui permet de l'identifier, directement ou indirectement, est un renseignement personnel.

Elle s'applique également à toute personne à qui la Fondation confie des renseignements personnels dans le cadre de l'exécution d'un mandat ou d'un contrat de service.

4 Principes directeurs

Dans l'exercice de ses activités, la Fondation recueille et traite des renseignements personnels. Pour protéger les renseignements personnels qu'elle détient, elle s'engage à prendre les mesures appropriées en fonction de la nature et de la sensibilité des renseignements qu'elle détient. Les pratiques de la Fondation en matière de protection des renseignements personnels reposent sur les principes suivants :

4.1 Sécurité

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.

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 Nécessité

La Fondation ne recueille que les renseignements personnels qui sont nécessaires à l'exercice de ses activités. Le personnel de la Fondation n'accède qu'aux renseignements personnels auxquels il a besoin pour s'acquitter de ses tâches.

4.3 Rétention des données

Toutes les données sont conservées conformément au calendrier fourni ci-dessous 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.

Type de données	**Période de rétention**
Grands livres	Permanent
Relevés de dons	7 ans
Informations personnelles des employé-es	7 ans
Procès-verbaux des réunions du CA	Permanent

4.4 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).

4.5 Classification

La classification des données s'applique à toutes les données 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.

La *Fondation* adopte les niveaux de classification de données suivants :

FONDATION DUFRESNE& GAUTHIER

4.5.1 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.

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

4.5.3 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.

4.6 Accès aux données

La Fondation 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 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.

4.7 Utilisation des données

Les employé-es, les contractuel-les et les bénévoles doivent accéder aux données 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.

4.7.1 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.

4.7.2 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.

4.7.3 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.

4.8 Destruction des données

La Fondation s'assure de détruire les renseignements personnels qu'elle détient lorsque les finalités sont accomplies, sous réserve des délais prévus à son calendrier de conservation (voir section 5.2).

FONDATION DUFRESNE& GAUTHIER

5 Rôles et responsabilités

5.1 Le conseil d'administration

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

Responsabilités:
Le conseil d'administration :

5.1.1 S'assure que des politiques encadrant la gestion des données sont mises en place au sein de la Fondation et que les ressources nécessaires sont allouées à leur mise en œuvre;

5.1.2 Révise et adopte les politiques encadrant la gestion des données;

5.1.3 Évalue les risques liés aux données : 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;

5.1.4 Surveille la conformité réglementaire en s'assurant que la Fondation 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 la Fondation s'adapte en conséquence;

5.1.5 S'assure que les politiques de gouvernance des données de la Fondation sont clairement communiquées à tous les employés, parties prenantes et autres personnes concernées. Il s'assure également que la Fondation est responsable de la gestion de ses données et est transparente dans ses activités liées aux données.

5.2 Responsable de la gouvernance des données

Le responsable de la gouvernance des données est chargé de superviser et de garantir que la Fondation se conforme aux lois et réglementations applicables en matière de protection des données personnelles. Il est également responsable de sensibiliser les employés de la Fondation à l'importance de la protection des données et de mettre en place les politiques et les procédures adoptées par le conseil d'administration pour assurer une saine gestion des données au sein de la Fondation. Il s'assure que les données collectées sont pertinentes pour les objectifs de la Fondation.

Responsabilités :
Le responsable de la gouvernance des données :

5.2.1 Surveille la conformité réglementaire de la Fondation aux lois et réglementations applicables en matière de protection des données, notamment la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels dans le secteur privé*;

5.2.2 Élabore des politiques et des procédures pour assurer la protection des données personnelles de la Fondation et les soumet au conseil d'administration pour approbation. Ces politiques et procédures peuvent inclure des politiques de confidentialité, des procédures de contrôle d'accès et des protocoles de gestion des incidents;

5.2.3 Évalue les risques liés à la collecte, au stockage et à l'utilisation des données de l'organisation et met en place des mesures pour les atténuer;

5.2.4 S'assure que les mesures de sécurité appropriées sont en place pour protéger les données contre les accès non autorisés, les pertes ou les altérations;

5.2.5 Sensibilise le personnel de la Fondation à l'importance de la protection des données personnelles;

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

5.2.7 Respecter les politiques de la Fondation 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.

5.3 Utilisateur de données

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

Responsabilités

Les utilisateurs de données :

5.3.1 Prend connaissance et respecte les politiques de la Fondation 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;

5.3.2 Protègent les données contre l'accès non autorisé, la divulgation ou la perte en utilisant des mesures de sécurité appropriées et conformes aux politiques et procédures adoptées par la Fondation;

5.3.3 Signalent tout problème lié aux données, y compris les violations de données ou les préoccupations de sécurité, au responsable de la gouvernance des données de la Fondation.

6 Application

Cette politique doit être respectée par tous les employé-es, contractuel-les et bénévoles de la *Fondation Dufresne & Gauthier*. 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 : les membres du conseil d'administration de la Fondation Dufresne & Gauthier
Date d'entrée en vigueur : 30 octobre 2023

FONDATION DUFRESNE& GAUTHIER

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.