

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

1. INTRODUCTION

1.1 OBJECTIFS

En vertu des dispositions législatives en matière de protection des renseignements personnels, le Groupement forestier Montmagny-L'Islet (GFML) est responsable de la protection des renseignements personnels qu'il détient, que leur conservation soit assurée par le groupement lui-même ou par un tiers. Conséquemment, la présente politique vise à :

- Préciser les pratiques du (GFML) dans sa gestion des renseignements personnels ;
- Définir les rôles et les responsabilités de toute personne travaillant dans l'organisation à l'égard des renseignements personnels et uniformiser les pratiques en la matière ;
- Permettre aux membres du personnel de connaître et de comprendre les exigences légales et les principes de protection des renseignements personnels dans le cadre de l'exercice de leurs fonctions.

1.2 CHAMP D'APPLICATION

La présente politique s'applique à tous les membres du personnel, permanents, contractuels ou stagiaire ainsi qu'aux membres du conseil d'administration ou de tout comité qui en découle lorsqu'ils recueillent, utilisent, communiquent, conservent ou détruisent des renseignements personnels dans le cadre de leurs fonctions. Elle s'applique de la même manière aux tiers traitant des renseignements personnels pour le compte du GFML.

La politique s'applique à tous les renseignements personnels, quel que soit leur support, de leur collecte jusqu'à leur destruction.

1.3 DÉFINITIONS

Renseignement personnel : Tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier, tel que : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, le numéro de producteur, la date de naissance, le dossier d'employé ou les coordonnées bancaires.

Renseignement personnel sensible : Un renseignement personnel est sensible lorsque, par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée en raison de sa nature ou du contexte de son utilisation.

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

De manière non limitative, un renseignement personnel inclus dans les catégories suivantes doit généralement être considéré comme sensible, soit les renseignements :

- financiers;
- génétiques ou biométriques;
- concernant la santé;
- concernant la vie sexuelle ou l'orientation sexuelle;
- concernant les convictions religieuses ou philosophiques;

Renseignement anonymisé : Tout renseignement qui ne permet plus, et de façon irréversible, d'identifier directement ou indirectement la personne concernée.

Collecte : Désigne le fait de recueillir, d'acquérir ou d'obtenir des renseignements personnels auprès de toute source, y compris les tierces parties, par quelque moyen que ce soit.

Incident de confidentialité : L'accès, l'utilisation ou la communication non autorisée par la loi d'un renseignement personnel, la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

2. RÔLES ET RESPONSABILITÉS

2.1 RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La direction générale est la personne responsable de la protection des renseignements personnels. Elle doit veiller à ce que l'organisation soit conforme aux modalités de protection des renseignements personnels prévues par la loi tout au long de leur cycle de vie. Elle doit notamment :

- Assurer le traitement des demandes de communication ou de rectification relatives aux renseignements personnels;
- Assurer la protection des renseignements personnels tout au long de leur cycle de vie, soit de leur collecte jusqu'à leur destruction;
- Assurer le traitement de tout signalement d'incident de confidentialité ou désigner une personne au sein de l'organisation pour recevoir et traiter un incident de confidentialité au premier niveau;
- Effectuer les redditions de comptes requises en matière de protection des renseignements personnels, le cas échéant.
- Assurer la tenue des registres et inventaires en matière de protection des renseignements personnels;

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

- Veiller à la sensibilisation et à la formation du personnel sur les obligations et les bonnes pratiques en matière de protection des renseignements personnels.
- Voir à la mise en œuvre des mesures correctrices concernant les événements ayant mis ou qui auraient pu mettre en péril la protection des renseignements personnels;
- Prendre en compte la protection des renseignements personnels lors du développement d'un système d'information, d'une prestation électronique de services, de sondage auprès des membres et lors des activités de représentation ;

2.2 ÉQUIPE DE SOUTIEN EN GESTION DE LA CONFIDENTIALITÉ

La personne responsable de la protection des renseignements personnels est, par défaut, la personne chargée du suivi et du traitement des plaintes ou incidents de confidentialité ainsi que de la gestion des demandes liées aux renseignements personnels.

Malgré ce qui précède, cette personne peut désigner une équipe de soutien en gestion de la confidentialité, soit une équipe constituée de deux à trois membres du personnel qui l'accompagne dans le suivi et le traitement des plaintes et incidents de confidentialité et demandes. Cette équipe permet donc :

- D'évaluer la recevabilité des plaintes et assurer leur suivi ;
- D'assurer le traitement d'un incident de confidentialité, évaluer le préjudice et tenir un registre des incidents ;
- De traiter chaque plainte de façon équitable ;
- De soutenir la personne responsable de la protection des renseignements personnels dans toutes les étapes de suivi des incidents ;
- De soutenir la personne responsable de la protection des renseignements personnels dans les procédures de mise en œuvre de la présente politique ;

2.3 LES MEMBRES DU PERSONNEL

a) gestionnaire :

Tout gestionnaire a une responsabilité dans la collecte, l'utilisation, la communication, la protection, la conservation ou la destruction des renseignements personnels auxquels ses employés ont accès.

- Soutenir l'innovation de technologie qui améliore la sécurité des renseignements personnels ;

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

- Prendre en compte la protection des renseignements personnels lors du développement de tout nouveau service ou nouvelle activité ;

b) tout le personnel

Afin d'assurer le respect des obligations en matière de protection des renseignements personnels, chacun doit :

- Accéder uniquement aux renseignements personnels nécessaires à l'exercice de ses attributions et assurer le respect des mesures de protection applicables à ces renseignements ;
- Utiliser de bonnes pratiques lors de manipulation de données confidentielles ;
- Veiller à ce que les renseignements personnels utilisés dans le cadre de ses fonctions soient utilisés aux fins exclusives pour lesquelles ils sont collectés ;
- Aviser sans délai le responsable du traitement des incidents de confidentialité, s'il a des motifs de croire qu'un incident de confidentialité s'est produit ;
- Informer la personne responsable de la protection des renseignements personnels de toute nouvelle communication de renseignements personnels requise dans le cadre de ses fonctions et appliquer les recommandations formulées en vue de cette communication ;
- Participer aux activités de formation et de sensibilisation, aux évaluations des facteurs relatifs à la vie privée lorsque requis ainsi qu'aux collectes de renseignements requises aux fins de reddition de compte.

3. GESTION DES RENSEIGNEMENTS PERSONNELS – CYCLE DE VIE

3.1 COLLECTE

Le GFML ne collecte que les renseignements personnels qui sont nécessaires à l'exercice de ses fonctions sous réserve des exceptions prévues par la *Loi*.

3.2 CONSENTEMENT

Le GFML informe adéquatement toute personne de la collecte de renseignements qui la concernent, de l'utilisation qu'il en fera, à qui il communiquera ses renseignements et à quelle fin (le cas échéant). Il s'assure d'informer la personne concernée, au plus tard au moment de la collecte :

- Des fins auxquelles ces renseignements sont recueillis ;
- Des moyens par lesquels les renseignements sont recueillis ;
- Des droits d'accès et de rectification prévus par la loi ;

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

- De son droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis.

Le consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée.

Le consentement doit être demandé pour chacune de ses fins et ne peut être général ni englober plusieurs fins. La personne concernée doit pouvoir comprendre et choisir pour quelles fins elle désire consentir.

Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles la personne concernée a consenti.

Le GFML s'assure que le consentement est manifesté de façon expresse dès que le renseignement personnel concerné est sensible.

Le consentement peut être explicite ou implicite et peut être fourni directement par la personne ou par son représentant autorisé.

L'obtention d'un consentement explicite est privilégiée, que ce soit verbalement, par voie électronique ou par écrit. Toutefois le consentement implicite peut être raisonnablement déduit de l'action ou l'inaction d'une personne. Par exemple, le fait de fournir un nom et une adresse pour recevoir une publication ou un nom et un numéro de téléphone pour obtenir une réponse à une question est considéré comme un consentement implicite à la collecte d'information contenant des renseignements personnels. Pour déterminer le type de consentement approprié, la sensibilité des renseignements personnels, ainsi que les fins auxquelles ils sont recueillis sont considérés.

3.3 UTILISATION

Le GFML utilise les renseignements personnels qu'il détient uniquement aux fins pour lesquelles ils ont été recueillis à moins que la Loi l'autorise à faire autrement. Il conserve les renseignements seulement pour la durée nécessaire pour accomplir les fins déterminées.

3.4 COMMUNICATION SANS LE CONSENTEMENT DE LA PERSONNE CONCERNÉE

Le GFML peut divulguer certains renseignements personnels qu'il détient, sans le consentement de la personne concernée, lorsque la situation le requiert et que la Loi le permet.

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le GFML peut communiquer certains renseignements personnels qu'il détient à un membre du personnel du GFML lorsque ces renseignements sont nécessaires à l'exercice de ses fonctions.

Nul ne peut communiquer à un tiers les renseignements personnels qu'il détient sur autrui, à moins que la personne concernée n'y consente ou la loi ne le prévoie.

Le GFML peut communiquer certains renseignements personnels qu'il détient à des tiers fournisseurs de service et/ou partenaires. Les renseignements auxquels accèdent ces fournisseurs de services se limitent à ceux nécessaires pour leur permettre de s'acquitter de leurs fonctions. De plus, les contrats conclus entre le GFML et ces fournisseurs de services exigent d'eux qu'ils préservent la confidentialité de ces renseignements et qu'ils y appliquent les dispositions de protection des renseignements personnels conformément à la loi.

Le GFML peut communiquer certains renseignements personnels à des fins d'étude, de recherche ou de production de statistiques sous réserve des conditions prévues par la Loi. Il pourrait aussi être tenu de partager certains renseignements personnels en réponse à une ordonnance d'un tribunal, à une assignation à témoigner ou à un mandat de perquisition du gouvernement, ou autrement pour collaborer avec de telles autorités gouvernementales et de tels organismes d'application de la loi.

3.5 COMMUNICATION AVEC LE CONSENTEMENT DE LA PERSONNE CONCERNÉE

Le GFML peut communiquer certains renseignements personnels qu'il détient à une tierce personne et pour des fins spécifiques, s'il a obtenu le consentement valable de la personne concernée.

3.6 CONSERVATION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

Le GFML ne conserve les renseignements personnels qu'il détient que pour le temps nécessaire pour atteindre les fins pour lesquelles il les a collectés à moins d'autorisation ou d'exigence des lois ou de la réglementation applicable. Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, le GFML doit le détruire ou l'anonymiser pour l'utiliser aux fins d'intérêt public.

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Lorsque le GFML procède à la destruction de documents contenant des renseignements personnels, il s'assure de prendre les mesures de protection nécessaires visant à assurer la confidentialité de ceux-ci.

Le Groupement privilégie l'utilisation de renseignements personnels anonymisés lorsque possible.

3.7 PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le GFML met en place des mesures de sécurité physiques, organisationnelles, contractuelles et technologiques appropriées et raisonnables afin de protéger les renseignements personnels, peu importe le support sur lequel ils sont enregistrés, contre la perte ou le vol et contre l'accès, la divulgation, la copie, l'utilisation ou la modification non autorisés par la loi.

Les personnes qui travaillent pour le GFML ou en son nom doivent, notamment :

- Faire des efforts raisonnables pour minimiser le risque de divulgation non intentionnelle de renseignements personnels ;
- Prendre des précautions pour s'assurer que les renseignements personnels ne sont pas épiés, entendus, consultés ou perdus, particulièrement lorsqu'elles travaillent dans des locaux autres que les bureaux du GFML ;
- Prendre des mesures raisonnables pour protéger les renseignements personnels lorsqu'elles se déplacent d'un endroit à l'autre.
- Assurer de ne fournir à un tiers fournisseur que les renseignements personnels requis pour assurer sa prestation de services auprès du GFML.

3.8 DESTRUCTION

Le Groupement détruit de façon sécuritaire les renseignements personnels lorsque les fins pour lesquelles ils ont été recueillis sont accomplies sous réserve des lois applicables quant à leur conservation. Cette destruction inclue notamment l'élimination des versions électroniques et le déchetage des copies papier.

4 DROIT D'ACCÈS ET DE RECTIFICATION

4.1 DROIT D'ACCÈS À DES RENSEIGNEMENTS PERSONNELS

Toute personne qui en fait la demande a le droit d'accéder aux renseignements personnels la concernant détenus par le GFML, sous réserve des exceptions prévues par la Loi.

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Une demande d'accès ne peut être considérée que si elle est faite par écrit par une personne physique prouvant son identité à titre de personne concernée, à titre de représentante ou de représentant, d'héritière ou d'héritier ou de successible de cette dernière, à titre de liquidatrice ou de liquidateur de la succession, à titre de bénéficiaire d'assurance vie ou d'indemnité de décès, à titre de titulaire de l'autorité parentale ou à titre de conjoint ou de proche parent d'une personne décédée. Cette demande doit être adressée à la personne responsable de la protection des renseignements personnels du GFML.

Une demande d'accès déposée conformément aux modalités prévues ne peut être refusée, sauf si l'accès est susceptible de mener à la divulgation de renseignements d'une autre personne et que cette personne refuse de consentir à la divulgation de ceux-ci ou lorsque des restrictions juridiques s'appliquent. Dans un tel cas, le demandeur est informé de la raison pour laquelle les renseignements ne peuvent être divulgués.

4.2 DEMANDE DE RECTIFICATION

Toute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la Loi, exiger que le fichier soit rectifié. Une demande de rectification ne peut être considérée que si elle est faite par écrit par une personne physique ayant droit d'accès aux renseignements personnels tel que décrit à 4.1.

5.PROCESSUS DE TRAITEMENTS DES PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Un processus est établi afin que chaque personne se sentant lésée, ou jugeant non justifiée une demande d'information liée à sa vie privée, puisse déposer une plainte. De même, ce processus est valable pour toute personne qui a des motifs de croire qu'un incident de confidentialité s'est produit et que le GFML a fait défaut d'assurer la confidentialité des renseignements personnels qu'il détient.

Le GFML s'engage ainsi à assurer un traitement adéquat, uniforme et diligent des plaintes formulées à son endroit via une procédure équitable et transparente.

5.1 TRAITEMENT DES PLAINTES

5.1.1 Dépôt d'une plainte

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La plainte doit être faite sur le formulaire de plainte en annexe C ou, à défaut, contenir les renseignements suivants :

- nom de la plaignante ou du plaignant;
- coordonnées pour joindre cette personne;
- motifs de cette plainte et faits l'entourant.

Tout membre du personnel du GFML qui reçoit une plainte verbale doit informer la plaignante ou le plaignant du présent processus et l'inviter à faire parvenir sa plainte par écrit à la personne responsable de la protection des renseignements personnels.

5.1.2 Réception de la plainte

Lorsqu'une plainte est reçue, la personne responsable de la protection des renseignements personnels l'analyse et la traite après en avoir accusé réception auprès de son auteur.

Dans le cas d'une plainte recevable, l'accusé de réception contient les renseignements suivants :

- Le nom et les coordonnées de la personne responsable du traitement de la plainte;
- Dans le cas d'une plainte incomplète, un avis comportant une demande de complément d'information à laquelle la plaignante ou le plaignant doit répondre dans un délai fixé, à défaut de quoi la plainte est réputée abandonnée;
- Le délai dans lequel la plainte sera traitée, soit 30 jours de la réception de la plainte ou 30 jours suivant la réception du complément d'information demandé.

Dans le cas d'une plainte irrecevable, l'accusé de réception contient :

- Le nom et les coordonnées de la personne responsable du traitement de la plainte;
- La conclusion indiquant que la plainte est irrecevable et les motifs appuyant cette conclusion.

5.1.3 Analyse et gestion de la plainte

La personne responsable de l'accès aux documents et de la protection des renseignements personnels fait les vérifications nécessaires au traitement de la plainte.

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La personne responsable du traitement des incidents de confidentialité détermine s'il s'agit bien d'un incident de confidentialité à l'aide de la Grille d'aide à la décision jointe en annexe D. Si l'une des réponses aux questions est négative, il ne s'agit pas d'un incident de confidentialité et le signalement est clos.

La personne ayant fait le signalement tout comme le responsable de la protection des renseignements peut demander une révision qui sera alors faite par une équipe désignée à cette fin par la personne responsable des renseignements.

Même si la réponse s'avère négative, la collecte d'informations et l'analyse sont documentées au registre d'incident. (Annexe F)

Si les réponses aux questions sont affirmatives, il s'agit d'un cas avéré d'un incident de confidentialité.

6. INCIDENTS DE CONFIDENTIALITÉ

Le GFML a établi des procédures de gestion des incidents de confidentialité impliquant des renseignements personnels. Les membres du personnel du GFML sont tenus de déclarer tout incident présumé ou avéré à la personne responsable de la protection des renseignements personnels.

6.1. GESTION DES INCIDENTS DE CONFIDENTIALITÉ

Lorsque le GFML a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel, il prend les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

Le GFML tient un registre des incidents de confidentialité, dont le contenu est déterminé par la Loi.

6.1.1 Évaluation du risque pour la personne concernée

Si elle considère qu'il s'agit bien d'un incident de confidentialité imputable au GFML, la personne responsable du traitement des incidents de confidentialité évalue le risque pour la personne concernée par le fait de l'incident. À cette fin, le ou la responsable du traitement des incidents de confidentialité établit le niveau du préjudice, en considérant les critères suivants :

- La sensibilité des renseignements personnels en cause;
- Le risque de réutilisation des renseignements personnels
- L'impact potentiel de l'incident sur la personne concernée;

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

- Le nombre de personnes concernées
- Le potentiel de survenance du préjudice;
- La vulnérabilité des personnes en cause.

6.2. NOTIFICATION DE L'INCIDENT

En présence d'un risque de préjudice sérieux, le responsable de la protection des renseignements personnels au sein du GFML signale la survenance d'un incident et des mesures correctives prises pour y remédier en diffusant les avis suivants.

6.2.1 L'avis à la Commission d'accès à l'information du Québec (CAI)

L'avis à la CAI doit être fait avec diligence. La personne responsable de la protection des renseignements personnels au sein du GFML formule l'avis à la CAI et lui transmet. Le contenu de l'Avis à la CAI se trouve en annexe H.

6.2.2. Avis à la personne concernée

L'avis à la personne concernée doit être fait avec diligence. La personne responsable de la protection des renseignements personnels au sein du GFML formule l'avis à la personne concernée et lui transmet. Le contenu de l'Avis à la personne concernée se trouve en annexe.

Cet avis se fait par tout moyen adéquat. Il peut s'agir d'un courriel ou d'une lettre postale. Toutefois, lorsqu'il est très difficile de joindre la personne directement, il est possible de recourir à un avis public. Le but est que la personne concernée ait ainsi indirectement connaissance de l'incident.

Le cas échéant, le ou la responsable de la protection des renseignements personnels au sein du GFML rédige et publie cet avis.

La personne responsable de la protection des renseignements personnels au sein du GFML n'est pas tenu d'aviser la personne concernée aussi longtemps que cet avis est susceptible d'entraver une enquête menée par un organisme chargé de prévenir, de détecter ou de réprimer une infraction aux lois.

6.3 EN L'ABSENCE D'UN PRÉJUDICE SÉRIEUX

La personne responsable de la protection des renseignements personnels au sein du GFML détermine s'il est pertinent d'informer de l'incident la personne concernée. Il peut choisir de le faire pour des raisons de transparence ou de gestion des affaires. Ces raisons sont documentées dans le registre des incidents de confidentialité.

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Si l'incident constitue un crime, la personne responsable de la protection des renseignements personnels au sein du GFML en informe le service de police compétent

6.4 CONSTITUTION D'UNE ÉQUIPE D'URGENCE POUR LE TRAITEMENT D'UN INCIDENT DE CONFIDENTIALITÉ

À tout moment et selon le degré de gravité, la personne responsable de la protection des renseignements personnels au sein du GFML peut mettre en place une équipe dédiée au traitement d'un incident de confidentialité spécifique. Constituée d'un minimum de trois membres, l'équipe d'urgence comprend la personne responsable de la protection des renseignements personnels, un autre cadre dirigeant et une autre ressource humaine pertinente pour l'avancement du processus.

L'équipe d'urgence a comme mandat de soutenir la personne responsable de la protection des renseignements personnels, pour l'analyse, les mesures correctives et le suivi d'un incident de confidentialité. Elle doit notamment :

- Déterminer les mesures correctives (mesures de mitigation immédiates) afin de contenir l'incident et d'en limiter les torts ou dommages, et s'assure de leur application ;
- Le cas échéant, faire intervenir les intervenants et les autorités externes pour trouver les solutions à la gestion de l'incident de confidentialité et les appliquer (policiers, assureurs, spécialistes, etc.);
- Déterminer les Mesures correctives (mesures de mitigation) afin de faire cesser l'incident, incluant le recours à toute personne susceptible de diminuer le préjudice, et s'assure de leur application ;
- Mesures préventives (mesures de mitigation supplémentaires) afin de faire en sorte que l'incident ne se reproduise pas.
- Coordonner les communications internes et externes, dont les avis publics, et notifier l'incident à la Commission d'accès à l'information (CAI), à la personne concernée et, au besoin, au ministère concerné, en utilisant l'avis public ;
- Mettre en place les mesures visant à réduire les impacts d'un incident de confidentialité sur la réputation du GFML.

Selon la gravité, l'équipe d'urgence PRP peut recommander l'octroi d'un mandat a un consultant externe.

POLITIQUE RELATIVE A LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

7. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption et demeure effective tant et aussi longtemps qu'elle n'est pas abrogée ou remplacée.