



Politique et documents

Loi sur la protection des renseignements
personnels dans le secteur privé

LE 
BLANC

Table des matières

2

1. Politique, formulaires, procédures et méthodes.....	4
Politique sur la gouvernance des renseignements personnels (confidentialité)	5
1.1 Formulaire de consentement à la collecte de renseignements personnels	21
1.2 Formulaire pour le consentement à la communication de renseignements personnels à un tiers (transparence).....	26
1.3 Formulaire de plainte.....	29
1.4 Lettre de consentement par la personne concernée à la communication de renseignements personnels	32
1.5 Procédure en cas d'incident de confidentialité	33
1.6 Procédure de traitement des plaintes.....	37
1.7 Méthode de destruction de renseignements personnels	38
1.8 Demande de la personne concernée pour avoir accès à ses renseignements personnels	39
1.9 Demande de la personne concernée pour la rectification ou suppression de ses renseignements personnels.....	41
1.12 Lettre d'acceptation de la demande d'accès de la personne concernée ...	43
1.13 Lettre de refus d'accès aux renseignements personnels	44
1.14 Lettre accusée réception d'une plainte.....	45
1.15 Lettre indiquant que la plainte est non recevable	46
1.16 Registre des incidents de confidentialité	48
1.17 Avis aux personnes concernées concernant un incident de confidentialité	49
1.18 Le temps de conservation des renseignements personnels.....	51
1.19 Demande de retrancher, d'une liste nominative, des renseignements personnels.....	52

Avis

L'information présentée dans le présent document est de nature générale et est mise à votre disposition sans garantie aucune notamment au niveau de son exactitude ou de sa caducité. Cette information ne doit pas être interprétée comme étant un avis professionnel, un ou des conseils ou un avis juridique. Elle est présente qu'à titre informatif.

Droits d'utilisation

L'utilisation du présent document est réservée au client qui a une autorisation d'accès. Tous les droits de vente, reproduction et modification appartiennent à Leblanc et Associés.

Il est interdit de diffuser ce document sans le consentement écrit de Leblanc et Associés.

1. Politique, formulaires, procédures et méthodes

Politique sur la gouvernance des renseignements personnels (confidentialité)

1. Le préambule

Dans son exercice de gestion, Gestion DMJ doit recueillir, traiter et communiquer des renseignements jugés personnels. Dans ce cadre, Gestion DMJ désire mettre en place, en respect de la *Loi sur la protection des renseignements personnels dans le secteur privé, chapitre p-39.1*, les processus, les méthodes, les règlements, les politiques pour assurer que le recueil, le traitement, la communication, la protection et la destruction des renseignements personnels soient conformes à la législation en vigueur dans ce domaine, et ultimement, assurer l'absence de tout incident de confidentialité et dans le cas contraire avoir en place les processus nécessaires pour minimiser ou éliminer les préjudices sérieux.

2. Les objectifs de la politique

La présente politique vise les objectifs suivants :

- Respecter la *Loi sur la protection des renseignements personnels dans le secteur privé, chapitre p-39.1* ;
- Protéger les renseignements personnels présents ;
- Réagir avec efficacité et démontrer la diligence de Gestion DMJ ;
- Comprendre ce qu'est un renseignement personnel ;
- Définir clairement les responsabilités et les obligations de chaque intervenant dans l'organisation ;
- Avoir en place les politiques et pratiques pour protéger les renseignements personnels détenus par Gestion DMJ ;
- Établir les actions à entreprendre dans le cas d'un risque d'incident de confidentialité sans préjudice sérieux ;

- Établir les actions à entreprendre dans le cas d'un incident de confidentialité avec un risque de préjudice sérieux ;
- Établir les modes de destructions sécuritaires de renseignements personnels ;
- Établir les règles de conservation des renseignements personnels.

3. Les définitions importantes

- **Employeur** : Gestion DMJ
- **Employé(e)** : Personne qui travaille pour l'employeur moyennant rémunération.
- **Cadre** : Signifie toute personne qui supervise des employé(e)s sous sa responsabilité.
- **Loi** : Loi sur la protection des renseignements personnels dans le secteur privé, chapitre P-39.1.
- **Renseignement personnel** : Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.
- **CAI** : Commission d'accès à l'information.
- **Règlement** : Règlement sur les incidents de confidentialité.
- **Registre** : Registre des incidents de confidentialité.
- **Anonymiser** : Processus irréversible par lequel les renseignements personnels sont traités de manière à rendre impossible l'identification directe ou indirecte de la personne concernée.
- **Personne concernée** : Personne physique qui est concernée par des renseignements personnels qui permettent, directement ou indirectement, de l'identifier.
- **La personne responsable** : Personne physique de qui relèvent les responsabilités de l'application et du respect de la Loi.
- **ÉFVP** : Évaluation des facteurs relatifs à la vie privée.

- 
- **Renseignement personnel sensible** : Un renseignement personnel est considéré comme sensible étant donné sa nature, entre autres médicale, biométrique ou autrement intime 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.
 - **Préjudice sérieux** : Un préjudice sérieux est un préjudice du fait de la sensibilité des renseignements personnels, des conséquences de leur utilisation et de la probabilité qu'ils soient utilisés, est préjudiciable envers la personne concernée.
 - **Incident de confidentialité** : Un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisée par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.
 - **Transaction commerciale** : Une transaction commerciale est l'aliénation ou la location de tout ou d'une partie d'une entreprise ou des actifs dont elle dispose, d'une modification de sa structure juridique par fusion ou autrement, de l'obtention d'un prêt ou de toute autre forme de financement par celle-ci ou d'une sûreté prise pour garantir l'une de ses obligations.
 - **Liste nominative** : Une liste nominative est une liste de noms, de numéros de téléphone, d'adresses géographiques, de personnes physiques ou d'adresses technologiques où une personne physique peut recevoir de la communication d'un document ou d'un renseignement technologique.
 - **Le droit de gérance** : Droit de l'employeur à mettre en place des mécanismes lui permettant de contrôler la gestion à tous les niveaux des renseignements personnels, du recueil à la destruction des renseignements personnels.
 - **Processus disciplinaire (Les mesures disciplinaires)** : Mesures imposées dans le but de corriger le comportement répréhensible d'un(e) employé(e). Le comportement répréhensible se manifeste notamment lorsqu'un(e) employé(e) ne se conforme pas aux devoirs de conduite inhérents aux fonctions et aux responsabilités du poste qu'il(elle) occupe, à une loi, à une politique ou à une directive en vigueur.

4. L'engagement de l'organisation

Gestion DMJ s'engage à assurer la protection des renseignements personnels qu'elle détient, acquiert, traite, transmet et détruit.



5. Le rôle et les responsabilités des membres du personnel et des cadres

Chaque membre du personnel et cadre ont la responsabilité de protéger et d'utiliser à bon escient les renseignements personnels accessibles dans le cadre du travail tout au long du cycle de vie des renseignements personnels.

En aucun temps, le membre du personnel ou le cadre ne recueillera, ne consultera, ne transmettra ou ne détruira des renseignements personnels sans avoir au préalable reçu la permission du responsable de la protection des renseignements personnels ou en cas d'absence, de son remplaçant.

Le non-respect de cette obligation pourrait engager un processus disciplinaire pouvant se traduire par un congédiement.

5.1 Le cycle de vie d'un renseignement personnel

Selon la Commission sur l'accès à l'information, le cycle de vie d'un renseignement personnel est le suivant :

- a. Collecte du renseignement personnel
- b. Utilisation du renseignement personnel
- c. Communication du renseignement personnel
- d. Conservation du renseignement personnel
- e. Destruction du renseignement personnel

6. Le rôle et les responsabilités du responsable de la protection des renseignements personnels tout au long du cycle de vie des renseignements personnels

La personne responsable de la protection des renseignements personnels doit :

- Définir son rôle et ses responsabilités au sein d'une politique ;
- Faire l'inventaire des renseignements personnels détenus et évaluer leur sensibilité ;

- Mettre en place des mesures pour prévenir ou limiter les conséquences d'un incident de confidentialité impliquant un renseignement personnel ;
- Réaliser les évaluations des facteurs relatifs à la vie privée (ÉFVP). L'ÉFVP est un processus qui sert à déterminer l'incidence que pourrait avoir un programme ou un service sur la vie privée d'une personne ;
- Sensibiliser et former le personnel de l'entreprise ;
- Assurer la gestion des incidents de confidentialité et tenir un registre de ces derniers ;
- Connaître la nature des renseignements personnels que Gestion DMJ possède ;
- Détenir, traiter et communiquer les renseignements personnels selon les règles édictées par la Loi ;
- Savoir qui peut avoir accès à ces renseignements personnels et pour quels motifs ;
- S'assurer que les renseignements personnels dont les personnes ont accès sont exigés dans le cadre de leurs fonctions ;
- Produire et mettre en place des politiques et des pratiques qui encadrent la gouvernance des renseignements personnels ;
- Appliquer ou faire appliquer les politiques et pratiques en matière de renseignements personnels.

7. La collecte de renseignements personnels

La collecte de renseignements personnels doit se faire en suivant les 3 règles suivantes :

- La règle du consentement ;
- La règle de l'intérêt sérieux et légitime et de la nécessité ;
- La règle de la cueillette directe.

7.1 La règle du consentement

Pour toute collecte de renseignements personnels, le consentement de la personne concernée est nécessaire. Les obligations suivantes doivent être respectées :

- Le consentement de la personne concernée doit être manifeste, libre et éclairé et donné à des fins spécifiques ;
- Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé ;
- Tout consentement devra être demandé pour chacune de ses fins, en termes simples et clairs ;
- Lorsque la demande de consentement sera faite par écrit, elle devra être présentée distinctement de toute autre information communiquée à la personne concernée ;
- Sauf exception prévue à la Loi, un renseignement personnel ne pourra être utilisé à une autre fin que celle prévue, à moins que la personne concernée n'y consente ;
- Le consentement doit être formulé de manière expresse avant d'utiliser un renseignement personnel sensible à une fin différente de celle prévue lors de la collecte.

De plus, pour respecter la notion de transparence prévue à la Loi lors de la collecte, les informations suivantes devront être transmises à la personne concernée :

- Les fins de la collecte ;
- Les moyens de la collecte ;
- Les droits d'accès et de rectification ;
- Le droit des personnes concernées de retirer leur consentement.
- Du nom du tiers ou des catégories de tiers pour qui la collecte est faite ;
- Du nom des tiers à qui il est nécessaire de communiquer les renseignements ;
- De la possibilité, selon le cas, que les renseignements soient communiqués à l'extérieur du Québec.
- Si la personne concernée en fait la demande, les informations suivantes devront lui être transmises :
 - Des renseignements personnels recueillis auprès d'elle ;

- Des catégories de personnes qui ont accès à ces renseignements au sein de l'organisation ;
- De la durée de conservation de ces renseignements ;
- Des coordonnées du responsable de la protection des renseignements personnels.



Le tout rédigé dans des termes simples et clairs sans considérer le moyen utilisé pour recueillir les renseignements.

7.2 La règle de l'intérêt sérieux et légitime et la notion de nécessité

La cueillette de renseignements personnels doit être faite dans un contexte d'un intérêt sérieux, légitime et lors de la constitution d'un dossier, l'objet doit y être inscrit.

7.2.1 La notion de nécessité

Les renseignements personnels qui peuvent être collectés sont ceux nécessaires à l'objet du dossier, c'est-à-dire uniquement si la finalité poursuivie est légitime, importante, urgente et réelle et si l'atteinte au droit à la vie privée consécutive à la collecte de chaque élément de renseignement est proportionnelle à cette finalité. La simple utilité d'un renseignement ne le rend pas nécessaire.

Spécifiquement, la nécessité est constatée si ces critères sont respectés :

- L'objectif poursuivi par la collecte de ces renseignements est réel, important et légitime.
- La collecte est rationnellement liée à cet objectif.
- Il n'existe pas d'autre solution raisonnable portant moins atteinte à la vie privée de la personne.
- L'effet utile est plus grand que le préjudice susceptible d'être causé à la personne.

7.2.2 En cas de doute sur la nécessité

En cas de doute sur sa nécessité, un renseignement personnel est réputé non nécessaire et ne doit pas être collecté.

7.3 La cueillette des renseignements personnels

7.3.1 La règle de la cueillette directe

Les renseignements personnels doivent être recueillis auprès de la personne concernée directement.

8. L'utilisation des renseignements personnels

8.1 L'utilisation

Les renseignements personnels ne peuvent être utilisés que pour la fin pour laquelle ils ont été collectés. Dans le cas où les renseignements personnels seraient utilisés pour une autre fin, l'autorisation de la personne concernée devra être donnée avant l'utilisation des renseignements personnels.

Comme il est prévu à la Loi, la collecte des renseignements personnels donne l'autorisation de la part de la personne concernée d'utiliser les renseignements collectés. Spécifiquement, les limites de l'utilisation des renseignements personnels sont les suivantes :

- Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour les recevoir au sein de l'organisation lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions ;
- Limiter l'utilisation des renseignements personnels : à moins d'une exception prévue par la loi, le consentement doit être obtenu de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli.

8.2 La sécurité lors de l'utilisation

Pendant l'utilisation des renseignements personnels, la personne qui en fait usage doit obligatoirement en assurer la protection. La personne doit, sans s'y restreindre.

- Ne pas donner accès aux renseignements personnels à une personne qui n'y est pas autorisée ;
- Dans le cas où la personne qui utilise les renseignements personnels quitte temporairement son espace de travail, les renseignements personnels doivent être disposés de manière à ne pas être à la vue des passants :
 - Les renseignements personnels doivent être rangés dans un classeur ou tiroir barré ;
 - L'écran de l'ordinateur doit être verrouillé.

- S'assurer que les renseignements personnels ne puissent être vus de l'extérieur de son poste de travail ou de son bureau ;
- Lors de discussions traitant de renseignements personnels, celles-ci doivent se faire dans un lieu privé où la discussion ne peut être entendue par les personnes qui n'ont pas l'autorisation d'y avoir accès.

9. La communication de renseignements personnels

9.1 Le consentement à la communication

Avant toute communication, qu'elle soit verbale ou écrite et par tous les moyen, téléphone, courriel, texto, lettre, rapport, site Web ou, etc., le consentement de la personne concernée est nécessaire sauf dans les cas prévus à la Loi.

Spécifiquement, les obligations suivantes doivent être respectées :

- Obtenir le consentement des personnes concernées pour communiquer leurs renseignements à un tiers (ex. : assureur ou prestataire de services), à moins d'une exception prévue par la Loi ;
- Respecter la règle du consentement ;
- Respecter les obligations prévues par la Loi lorsqu'elle communique des renseignements personnels sans le consentement de la personne concernée ;
- Respecter les obligations particulières applicables à la communication de renseignements personnels à l'extérieur du Québec.

L'autorisation de collecter et d'utiliser les renseignements personnels ne permet pas la communication à un tiers des renseignements en question.

La personne concernée devra remplir et signer le formulaire, *consentement à la communication*.

10. Utilisation de renseignements personnels sans le consentement de la personne visée

La transmission de renseignements personnels sans le consentement de la personne concernée est possible dans les cas suivants :

- Au directeur des poursuites criminelles et pénales si le renseignement est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec ;
- À un organisme chargé, en vertu de la loi, de prévenir, détecter ou réprimer le crime ou les infractions aux lois qui le requiert dans l'exercice de ses fonctions, si le renseignement est nécessaire pour la poursuite d'une infraction à une loi applicable au Québec ;
- À une personne à qui il est nécessaire de communiquer le renseignement dans le cadre d'une loi applicable au Québec ou pour l'application d'une convention collective ;
- À un organisme public au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements publics et sur la protection des renseignements personnels qui, par l'entremise d'un représentant, le recueille dans l'exercice de ses attributions ou la mise en œuvre d'un programme dont il a la gestion ;
- À une personne ou à un organisme ayant le pouvoir de contraindre leur communication et qui les requiert dans l'exercice de ses fonctions ;
- À une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée ;
- À des tiers en vue de prévenir un acte de violence, dont un suicide et lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence ;
- À un service d'archives dans certaines conditions et/ou après un certain délai ;
- À une personne qui peut utiliser ce renseignement à des fins d'étude, de recherche ou de productions de statistiques conformément à l'article 21 ou à une personne qui est autorisée conformément à l'article 21.1 de la Loi ;
- À une personne qui, en vertu de la loi, peut recouvrer des créances pour autrui et qui le requiert à cette fin dans l'exercice de ses fonctions ;
- À une personne si le renseignement est nécessaire aux fins de recouvrer une créance de l'entreprise ;

- À toute personne ou tout organisme susceptible de diminuer un risque suivant un incident de confidentialité impliquant un renseignement personnel, en ne lui communiquant que les renseignements personnels nécessaires à cette fin ;
- Dans le cas d'une transaction commerciale ;
- Dans le cas d'une demande pour une liste nominative.

11. L'incident de confidentialité

11.1 La procédure en cas d'incident de confidentialité

Dans le cas où un incident de confidentialité avec ou sans risque de préjudice sérieux, la procédure portant le nom de *Procédure en cas d'incident de confidentialité*, doit être suivie.

12. Le traitement des plaintes relatives à la protection des renseignements personnels

12.1 Le traitement des plaintes

Le traitement adéquat, uniforme et diligent des plaintes est une priorité chez Gestion DMJ. Toute personne insatisfaite du processus de collecte, d'utilisation, de communication ou de destruction de renseignements personnels peut déposer une plainte à la personne responsable de la protection des renseignements personnels.

12.2 Le processus de traitement d'une plainte.

Dans le cas où une plainte est déposée, le responsable de la protection des renseignements personnels doit suivre les étapes prévues à la *Procédure de traitement d'une plainte*. Il bénéficie de 30 jours pour le faire. Les étapes suivantes devront être suivies :

- a) Réception de la plainte
- b) Analyse de la recevabilité
- c) Si la plainte est non recevable
 - i. Lettre à la personne plaignante et arrêt du processus
- d) Si la plainte est recevable
 - ii. Lettre à la personne plaignante et enquête

- e) Enquête
- f) Résultat de l'enquête
- g) Avis écrit à la personne plaignante sur le résultat de l'enquête
- h) Mise en place des solutions

La personne responsable prendra toutes les actions pour protéger au maximum les renseignements personnels détenus, traités et communiqués.

12.3 Les mesures de sécurité

La personne responsable devra mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits.

Ces mesures sont raisonnables compte tenu notamment de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

13. La conservation des renseignements personnels

Le responsable de la protection des renseignements personnels verra à la conservation des renseignements personnels. La conservation consiste en la période de temps pendant laquelle sont conservés les renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

13.1 Les règles de conservation

Il s'agit spécifiquement :

- Assurer la mise à jour et l'exactitude des renseignements personnels détenus au moment où ils sont utilisés pour une décision relative à la personne concernée ;
- Mettre en place et respecter les mesures nécessaires pour assurer la sécurité des renseignements personnels ;
- Conserver les renseignements personnels jusqu'à l'atteinte de la finalité pour laquelle ils ont été collectés ou selon les modalités déterminées par une loi ;
- Conserver les renseignements personnels dans un endroit sécuritaire et prévu à cette fin ;

- Permettre l'utilisation des renseignements personnels lorsque la finalité pour laquelle ils ont été collectés est accomplie, qu'avec le consentement de la personne concernée, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement.

13.2 La fin de la durée de conservation

À la fin de la durée de conservation des renseignements personnels, soit à l'arrivée de la finalité pour laquelle ils ont été collectés, (nom de l'organisation) s'assurera :

- De les détruire de manière sécuritaire et comme prévu à la présente politique ;

Ou

- De les anonymiser (c'est-à-dire qu'ils ne permettent plus d'identifier la personne concernée ni d'établir un lien entre la personne concernée et les renseignements personnels) et ce de manière irréversible dans le but de les utiliser à des fins sérieuses et légitimes.

13.3 Le temps de conservation

Le temps de conservation est la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé ou celui prévu au document sur le *temps de conservation des renseignements personnels* ou celui prévu à une loi en vigueur.

14. Les règles de destruction des renseignements personnels

Le responsable de la protection des renseignements personnels doit s'assurer que la destruction des renseignements personnels se fasse de manière sécuritaire. De plus, si l'organisation désire garder les renseignements personnels, le responsable de la protection des renseignements personnels devra en assurer l'anonymisation et l'utilisation à des fins sérieuses et légitimes.

14.1 Le moment de la destruction

Le responsable de la protection des renseignements personnels devra faire en sorte et prendre les mesures nécessaires lorsque la finalité pour laquelle les renseignements personnels ont été collectés est accomplie, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement (ex. pour des obligations fiscales), qu'ils soient détruits.

14.2 Les méthodes de destruction

Une méthode de destruction est un processus qui permet de détruire de manière permanente et irréversible des renseignements personnels. Il peut s'agir de déchiqueter, formater, réécrire, destruction physique, broyage, démagnétisation, écrasement d'information. Les pratiques sont prévues au document *Méthode de destruction de renseignements personnels*.

14.3 Les méthodes d'anonymisation

Une méthode d'anonymisation est un processus irréversible par lequel les renseignements personnels sont traités de manière à rendre impossible l'identification directe ou indirecte de la personne concernée.

15. L'accès et la rectification des renseignements personnels

15.1 Le droit à un accès aux renseignements personnels

En tout temps, à la suite d'une demande, les personnes concernées peuvent demander l'accès au responsable de la protection des renseignements personnels à leurs renseignements personnels détenus par Gestion DMJ. Pour ce faire, la personne concernée devra remplir le formulaire de *Demande d'accès aux renseignements personnels* et le faire parvenir au responsable de la protection des renseignements personnels.

Une lettre informant la personne concernée lui sera envoyée l'informant de l'acceptation de sa demande d'accès à ses renseignements personnels (*Lettre d'acceptation de la demande d'accès*)

15.2 La décision quant à l'accès aux renseignements personnels

Le responsable de la protection des renseignements personnels devra donner suite à la demande d'accès en acceptant ou en refusant la demande dans les 30 jours de la date de réception du formulaire d'accès aux renseignements personnels. L'absence de réponse de la part du responsable de la protection des renseignements personnels, à l'expiration du délai, équivaut à un refus.

15.2.1 Le droit de refuser l'accès

Le droit d'accès n'est pas absolu et comporte certaines restrictions.

De manière générale, le responsable de la protection des renseignements personnels peut refuser à la personne concernée d'avoir accès à ses renseignements personnels lorsque la divulgation de ces renseignements risquerait vraisemblablement :

- De nuire à une enquête ;
- D'avoir un effet sur une procédure judiciaire dans laquelle l'une ou l'autre de ces personnes a un intérêt ;

Et

- Lorsque la divulgation révélerait un renseignement personnel sur un tiers ou encore l'existence d'un tel renseignement et que cette divulgation serait susceptible de nuire sérieusement à ce tiers ;

De plus,

- La personne responsable de la protection des renseignements personnels doit refuser de communiquer un renseignement personnel :
 - Au liquidateur de la succession,
 - Au bénéficiaire d'une assurance-vie ou d'une indemnité de décès,
 - À l'héritier ou au successible de la personne concernée par ce renseignement,

à moins que cette communication ne mette en cause les intérêts et les droits de la personne qui le demande à titre de liquidateur, de bénéficiaire, d'héritier ou de successible.

Une lettre informant la personne concernée du refus lui sera envoyée. (*voir : Lettre de refus d'accès aux renseignements personnels*).

15.3 Le droit à la rectification

Toute personne concernée a le droit de demander au responsable de la protection des renseignements personnels une rectification des renseignements personnels la concernant (*Demande de rectification ou suppression des renseignements personnels par la personne concernée*).

Le responsable de la protection des renseignements personnels devra faire parvenir une réponse à la personne concernée de manière diligente, dans les 30 jours de la réception de la demande de rectification soumise par celle-ci.

L'absence de réponse dans ce délai équivaut à un refus.

15.4 L'application de la politique

Le responsable de la protection des renseignements personnels a la responsabilité d'interpréter et d'appliquer la politique.

15.5 Révision de la politique

La présente politique sera révisée tous les 3 ans.

15.6 La date d'entrée en vigueur

La politique entrera en vigueur le 22 septembre 2023.

1.1 Formulaire de consentement à la collecte de renseignements personnels

21

En conformité avec l'article 14 de la *Loi sur la protection des renseignements personnels dans le secteur privé*. Le présent formulaire vise à ce que le consentement de la personne concernée soit libre, éclairé et être donné à de fins spécifiques et à confirmer que le consentement qui ressort du présent formulaire ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

Section 1. Identité de la personne concernée par les renseignements personnels

Prénom et nom

Adresse

Ville

Code postal

Téléphone

Courriel

()

Section 2. Identité de la personne responsable de la protection des renseignements personnels qui demande la collecte des renseignements personnels

(à compléter par la personne responsable de la protection des renseignements personnels qui demande la collecte des renseignements personnels)

Prénom et nom

Nom de l'organisation

Adresse de l'organisation

Ville

Code postal	Téléphone ()	Courriel
-------------	------------------------	----------

Section 3. Les renseignements personnels visés par la demande de consentement

Les renseignements personnels suivants sont visés par la demande :

3.1. Existe-t-il des renseignements personnels dans la liste précédente que vous désirez ne pas inclure dans votre consentement ?

- ☐ Non
- ☐ Oui, les suivants :

Section 4. : La collecte de renseignements personnels

(à compléter par la personne responsable de la protection des renseignements personnels qui demande la collecte les renseignements personnels)

La collecte des renseignements personnels est nécessaire aux fins de (indiquer les besoins qui motivent la collecte) :

Les moyens de la collecte des renseignements personnels utilisés sont (indiquer les besoins et les moyens utilisés pour la collecte) :

Section 5. Les droits d'accès et de rectification

Pendant le processus de collecte, d'utilisation et de communication, la personne concernée a un droit d'accès et de rectification des renseignements personnels que détient Gestion DMJ sur son sujet. Les stipulations de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Section 6. Le droit des personnes concernées de retirer leur consentement

Pendant le processus de collecte, d'utilisation et de communication, la personne concernée a le droit de retirer son consentement en suivant les stipulations de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Section 7. Informations sur les tiers à qui pourraient être communiqués les renseignements personnels de la personne concernée selon le cas

(à compléter par la personne responsable de la protection des renseignements personnels qui demande la collecte des renseignements personnels)

Il est important de mentionner qu'aucune communication des renseignements personnels de la personne concernée ne sera transmise sans l'autorisation écrite de la personne concernée en respectant les obligations prévues à la *Loi sur la protection des renseignements personnels dans le secteur privé*.

- ☐ Les renseignements personnels seront utilisés uniquement par Gestion DMJ sous le contrôle de Kevin Massé, associé ;
- ☐ Nom du tiers ou des catégories de tiers pour qui la collecte est faite :
- ☐ Nom des tiers à qui il est nécessaire de communiquer les renseignements :
- ☐ Il est possible que les renseignements soient communiqués à l'extérieur du Québec.

Nom des tiers à qui pourraient être communiqués les renseignements personnels à l'extérieur du Québec :

Section 8. Durée du consentement

Ce consentement est valide, après ma signature de ce document, pour une durée de :

- ☐ Le temps nécessaire aux fins pour lesquelles il a été demandé
- ☐ Pour la durée suivante : _____

Passé un délai d'un an, une nouvelle entente devra être signée.

Section 9. Protection des renseignements personnels

Les renseignements personnels qui seront collectés sont nécessaires aux fins de la réalisation mentionnée dans le présent formulaire. Tous les renseignements seront traités avec la plus grande discrétion et confidentialité possible. La personne responsable de la protection des renseignements personnels qui contrôlera les renseignements personnels collectés de manière à ce qu'ils ne soient utilisés que pour les fins pour lesquelles ils sont nécessaires.

Signature de la personne responsable de la protection des renseignements personnels.

Signature

Section 10. Consentement à la collecte de renseignements personnels de la personne concernée

Par la présente signature, je confirme mon consentement manifeste, libre, éclairé et je suis informé des fins spécifiques pour lesquelles il est donné.

J'ai lu et je comprends la portée de ce document

Date

Signature de la personne concernée

1.2 Formulaire pour le consentement à la communication de renseignements personnels à un tiers (transparence)

26

Section 1. Identité de la personne concernée par les renseignements personnels

Prénom et nom

Adresse

Ville

Code postal

Téléphone

Courriel

()

Section 2. Consentement à la communication

Je, _____, consens à ce que Kevin Massé, associé au nom de Gestion DMJ communique à la personne désignée à la Section 4, les renseignements qu'il détient relativement à ce qui suit (indiquer le ou les documents visés) :

Section 3. Durée du consentement

Ce consentement est valide, après ma signature de ce document, pour une durée de :

☐ Le temps nécessaire aux fins pour lesquelles il a été demandé

☐ Pour la durée suivante : _____

Passé ce délai d'un an, une nouvelle entente devra être signée.

Il est entendu que je peux révoquer le consentement par simple avis au responsable de la protection des renseignements personnels.

Section 4. Renseignements sur l'identité de la personne (physique ou morale) désignée pour recevoir les renseignements personnels

(à compléter par la personne responsable de la protection des renseignements personnels qui communiquera les renseignements personnels)

Prénom et nom (personne désignée qui recevra les renseignements personnels)		Nom de l'organisme	
Adresse		Ville	
Code postal	Téléphone ()	Télécopieur ()	Courriel

Section 5. Protection des renseignements personnels

Les renseignements personnels qui seront communiqués et utilisés par la personne désignée pour la recevoir sont nécessaires aux fins de la réalisation de (indiquer le projet). Tous les renseignements seront traités avec la plus grande discrétion et confidentialité possible. La personne responsable de la protection des renseignements personnels qui transmettra les renseignements ne communiquera que les renseignements nécessaires aux fins du (indiquer le projet).

Signature de la personne responsable de la protection des renseignements personnels qui communiquera les renseignements.

Date

Signature

Section 6. Signature de la personne concernée

Par la présente signature, je confirme mon consentement manifeste, libre, éclairé et je suis informé des fins spécifiques pour lesquelles il est donné.

J'ai lu et je comprends la portée de ce document

Date

Signature

1.3 Formulaire de plainte

Information sur la personne plaignante
Prénom et nom :
Adresse :
Numéro de téléphone :
Adresse courriel :

Description de la plainte
Dates ou période concernant le ou les renseignements personnels :
Votre lien avec l'organisation (client, employé, fournisseur, etc.) :

La plainte :

Faits ou soutien de la plainte (veuillez joindre une copie des documents, nom des témoins, photos, vidéos, etc.):

Avez-vous déposé une plainte à la Commission d'accès à l'information :	() Oui Date :	() Non
J'atteste que les renseignements fournis dans ce formulaire sont, à ma connaissance, véridiques et complets. Prénom et nom :		
Signature :		Date :
J'autorise Kevin Massé, associé au nom Gestion DMJ à communiquer aux personnes impliquées, des renseignements personnels me concernant et des documents fournis au soutien de ma plainte. Ces renseignements ne seront communiqués que s'ils sont nécessaires au traitement de ma plainte, jusqu'à une décision finale. Par le fait même, je consens à ce que Kevin Massé, associé au nom Gestion DMJ utilise mes renseignements personnels pour l'analyse de ma plainte et pour l'enquête. La durée de mon consentement est la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.		
Prénom et nom :		
Signature :		Date :

1.4 Lettre de consentement par la personne concernée à la communication de renseignements personnels

32

(Ville et date)

(Nom du responsable dans l'entreprise)

(Coordonnées du responsable dans l'entreprise)

Objet : Consentement à la communication de renseignements personnels

Monsieur Kevin Massé, associé

Je soussigné(e) (prénom et nom), consens à ce que vous Kevin Massé, associé, au nom de Gestion DMJ, divulguiez, communiquiez et échangiez mes renseignements personnels pertinents contenus dans mon dossier détenu par votre organisation (nom de l'organisation) aux intervenants œuvrant pour (nom de l'organisation qui recevra les renseignements personnels).

En tout temps, je pourrai retirer mon consentement à la divulgation et à l'échange d'informations.

Signature de la personne concernée

Date

Signature de la personne faisant signer le formulaire

Date

1.5 Procédure en cas d'incident de confidentialité

1. Dès qu'une personne a des motifs de croire qu'un incident mettant en danger la confidentialité s'est produit, elle doit aviser la personne responsable.
2. Si la personne responsable détermine qu'il s'agit d'un incident de confidentialité, elle doit déterminer s'il existe un risque de préjudice sérieux. Pour ce faire, elle doit :

*Les étapes qui suivent peuvent être réalisées simultanément.

2.1 Évaluer la situation

- Établir les circonstances de l'incident (heure, jour, lieu, personne qui a rapporté l'incident, etc.) ;
- Identifier les renseignements personnels impliqués ;
- Identifier les personnes dont les renseignements personnels sont concernés ;
- Trouver la cause (erreur humaine, vulnérabilité informatique, perte, vol, etc.).

Cette évaluation doit se poursuivre tant que toutes les informations n'ont pas été identifiées.

2.2 Diminuer les risques

Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que d'autres incidents de même nature se produisent, par exemple :

- Cesser la pratique non autorisée ;
- Récupérer ou exiger la destruction des renseignements personnels impliqués ;
- Corriger les lacunes informatiques ;
- Inscrire une note dans les dossiers visés par un risque de vol d'identité ;
- Exiger des vérifications supplémentaires ;

- Révoquer ou modifier les mots de passe ou les codes d'accès informatiques.

2.3 Déterminer la nature du préjudice

Remplir le formulaire d'évaluation du préjudice (Formulaire d'évaluation du préjudice). En considérant le résultat du formulaire, la responsable de l'accès aux renseignements personnels détermine s'il y a absence ou présence d'un préjudice sérieux.

2.3.1 *Absence de risque préjudice sérieux*

Dans ce cas vous devez inscrire l'incident dans votre registre des incidents.

2.3.2 *Présence d'un risque de préjudice sérieux*

- Aviser dès que possible la Commission d'accès à l'information (CAI), même si l'ensemble des informations relatives à l'incident n'a pas encore été colligé ;
- Aviser les personnes concernées par avis direct et/ou avis public ;
 - i. L'avis direct est à privilégier (Annexe 3) ;
 - ii. L'avis public peut s'avérer nécessaire afin d'agir rapidement pour diminuer le risque de préjudice sérieux. Il doit être suivi d'un avis direct dès que les circonstances le permettent ;
 - iii. Seul un avis public est publié :
 - Lorsque le fait de transmettre l'avis est susceptible de causer un préjudice accru aux personnes concernées ;
 - Lorsque le fait de transmettre l'avis est susceptible de représenter une difficulté excessive pour vous ;
 - Lorsque vous n'avez pas les coordonnées des personnes concernées.

Un délai peut s'appliquer entre la connaissance de l'incident et l'avis aux personnes concernées. Ce délai peut être nécessaire pour compléter l'évaluation de la situation ou pour éviter d'entraver une enquête en cours par une personne ou un organisme qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

2.3.3 Aviser toute autre personne ou organisme susceptibles de diminuer le risque

- Expert en gestion et protection des renseignements personnels
- Expert en Cybersécurité
- Service de police
- Agences de crédit
- Banques
- Agences ou instances gouvernementales
- Ordre professionnel
- Syndicat
- Autres

Le consentement de la personne concernée par l'incident de confidentialité n'est pas requis. Le cas échéant, il est recommandé d'inscrire cette communication au registre des incidents de confidentialité afin de conserver une trace documentaire de celle-ci.

2.3.4 Inscrire l'incident de confidentialité au registre

- L'incident doit être inscrit au Registre des incidents de confidentialité.

3. Faire un suivi et prévenir tous futurs incidents de confidentialité

La personne responsable doit s'assurer :

- Que l'incident est clos ;
- Que le même incident ne se reproduira plus en considérant ce qui a été mis en place ;
- D'émettre, selon le cas, des recommandations aux supérieurs immédiats de l'organisation ou au conseil d'administration ;
- De mettre en place, selon le cas, des processus de prévention et de formation des acteurs impliqués ;

- S'assurer de la réelle nécessité de la collecte des renseignements personnels ;
- S'assurer que la durée de conservation des dossiers est de 5 ans de la connaissance de l'incident de confidentialité ;
- Réviser le plan d'intervention en continu.

1.6 Procédure de traitement des plaintes

Étapes	Délai	Interventions
(1) Réception de la plainte	Tout le processus d'enquête doit être terminé dans les 30 jours du dépôt de la plainte	Envoi d'un accusé de réception de la plainte
(2) Analyse de recevabilité L'analyse de recevabilité consiste à déterminer si, dans la mesure où toutes ou une partie des allégations de la plainte s'avèraient exactes, c'est-à-dire démontrées par preuve prépondérante, que cela pourrait constituer un manque en rapport à la gouvernance des renseignements personnels.		• L'objet de la plainte est en rapport avec les renseignements personnels. • La plainte vise une pratique prévue dans la politique de gouvernance. • L'analyse démontre que les faits reprochés pourraient constituer un manque en rapport avec la politique de gouvernance.
2.1 Si la plainte est non recevable		Envoi d'une lettre indiquant que la plainte n'est pas recevable.
2.2 Si la plainte est recevable, enquête		Envoi d'une lettre indiquant le début de l'enquête.
(3) Enquête		Rédaction du rapport d'enquête.
(4) Résultat de l'enquête		Rédaction du rapport d'enquête
(5) Avis écrit à la personne plaignante sur le résultat de l'enquête		Lettre indiquant le résultat de l'enquête et les modifications, selon le cas, qui seront mises en place.
(6) Mise en place des solutions		Mise en place de modifications.

1.7 Méthode de destruction de renseignements personnels

Support utilisé	Exemples de méthodes de destruction
Papier (original et toutes les copies)	Déchiqueteuse, de préférence à découpe transversale. Si les documents sont très confidentiels : déchiqueteuse + incinération.
Médias numériques que l'on souhaite réutiliser ou recycler Ex. cartes de mémoire flash (carte SD, XD, etc.) clés USB, disque dur d'ordinateur	Formatage, réécriture, déchiquetage numérique (logiciel effectuant une suppression sécuritaire et qui écrira de l'information aléatoire à l'endroit où se trouvait le fichier supprimé).
Médias numériques non réutilisables. Ex. certains CD, DVD, cartes de mémoire flash, clés USB et disques durs qui ne seront plus utilisés	Destruction physique (déchiquetage, broyage, meulage de surface, désintégration, trouage, incinération, etc.). La plupart des déchiqueteuses pourront détruire les CD et les DVD. Démagnétiseur pour les disques durs.
Machines contenant des disques durs. Ex., photocopieur, télécopieur, numériseur, imprimante, etc.	Écrasement des informations sur le disque dur ou disque dur enlevé et détruit lorsque les machines sont remplacées.

1.8 Demande de la personne concernée pour avoir accès à ses renseignements personnels

(Ville et date)

Monsieur Kevin Massé,

Associé

(Coordonnées du responsable dans l'entreprise)

OBJET : Demande d'accès à des renseignements personnels

Madame, Monsieur,

En vertu de l'article 27 de la Loi sur la protection des renseignements personnels dans le secteur privé, je désire recevoir une copie de tous documents me concernant, dont les suivants :

*(Indiquez le ou les document(s) vous concernant que vous désirez obtenir).
(Expliquez brièvement la situation ou le contexte et précisez, s'il y a lieu, le nom de l'entreprise qui détient le ou les document(s) contenant les renseignements personnels vous concernant).*

Vous en remerciant à l'avance, je vous prie d'agréer (Madame, Monsieur) mes salutations distinguées.

Signature :

Nom,
prénom :

Adresse :

Tél. jour : ()

1.9 Demande de la personne concernée pour la rectification ou suppression de ses renseignements personnels

41

(Ville et date)

Monsieur Kevin Massé

Associés

(Coordonnées du responsable dans l'entreprise)

OBJET : Demande de rectification à des renseignements personnels

Madame, Monsieur,

En vertu de l'article 28 ou 30 de la Loi sur la protection des renseignements personnels dans le secteur privé, je désire que vous (corrigiez ou supprimiez) :
_____ (indiquez le ou les renseignement(s) personnel(s)
visé(s) par la demande). (Expliquez brièvement la situation ou le contexte et précisez, s'il y a lieu, le nom de l'entreprise qui détient le ou les document(s) contenant les renseignements personnels vous concernant).

(Ajoutez les motifs justifiant la rectification et joindre, le cas échéant, les documents pertinents.)

42

Je vous remercie à l'avance et vous prie d'agréer (Madame, Monsieur), mes salutations distinguées.

Signature :

Nom,
prénom :

Adresse :

Tél. jour : ()

1.12 Lettre d'acceptation de la demande d'accès de la personne concernée

Ville et date

Nom du demandeur

Objet : Accès à vos renseignements personnels

Madame/Monsieur,

À la suite de votre demande d'accès à vos renseignements personnels contenus dans nos dossiers, la présente vise à vous informer que votre demande est acceptée.

Nous vous prions de communiquer avec le soussigné pour convenir du mode de transmission de vos renseignements personnels.

Veuillez croire, madame/monsieur, à nos distinguées salutations.

XXX XXXXX

Le responsable de la protection
des renseignements personnels

1.13 Lettre de refus d'accès aux renseignements personnels

Ville et date

Nom du demandeur

Objet : Refus d'accès à vos renseignements personnels

Madame/Monsieur,

À la suite de votre demande d'accès à vos renseignements personnels contenus dans nos dossiers, la présente vise à vous informer que votre demande est refusée.

La (les) raison(s) motivant le refus est(sont) que (indiquer la ou les raisons du refus)

Nous vous prions de communiquer avec le soussigné pour plus d'information.

Veuillez croire, madame/monsieur, à nos distinguées salutations.

XXX XXXXX

Le responsable de la protection
des renseignements personnels

1.14 Lettre accusée réception d'une plainte

Ville et date

Nom du demandeur

Objet : Accusé réception de votre plainte

Madame/Monsieur,

Nous accusons réception de votre plainte datée du (date). Votre plainte sera traitée conformément à notre politique de *Gouvernance des renseignements personnels*.

Vous serez informé à chaque étape du processus d'enquête. La première étape étant l'analyse de recevabilité de votre plainte.

Nous vous prions de communiquer avec le soussigné pour plus d'information.

Veuillez croire, madame/monsieur, à nos distinguées salutations.

XXX XXXXX

Le responsable de la protection
des renseignements personnels

1.15 Lettre indiquant que la plainte est non recevable

Ville et date

Nom du demandeur

Objet : Non-recevabilité de votre plainte

Madame/Monsieur,

Faisant suite à notre lettre datée du (date de la lettre) accusant réception de votre plainte, nous avons effectué, conformément à notre politique de *Gouvernance des renseignements personnels*, une analyse de recevabilité. Cette analyse vise à déterminer si les allégations contenues dans votre plainte pourraient en partie ou dans son ensemble s'avérer fondées, cela démontrerait une ou des entraves à la politique.

Pour prendre cette décision, nous avons tenu compte des facteurs suivants :

- Les plaintes concernent les renseignements personnels que l'organisation a en main ;
- Les renseignements personnels sont sur la personne plaignante ou une personne sous sa responsabilité ;
- La politique s'applique pour cette personne ;
- À première vue, les faits allégués et la preuve partielle soumise présentent une apparence suffisante d'une ou de plusieurs entraves à la politique et justifiant ainsi la poursuite du traitement de la plainte ;
- La plainte vise une ou des entraves prévues dans votre politique ;

Compte tenu de l'analyse des facteurs ci-haut mentionnés, nous devons vous aviser que votre plainte est non recevable.

Nous vous prions de communiquer avec le soussigné pour plus d'information.

Veuillez croire, madame/monsieur, à nos distinguées salutations.

XXX XXXXX

Le responsable de la protection
des renseignements personnels

1.16 Registre des incidents de confidentialité

REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ									
DATE DE L'ÉVÉNEMENT	DATE DE LA PRISE DE CONNAISSANCE	RENSEIGNEMENTS VISÉS	MESURES PRISES POUR DIMINUER LE RISQUE	NB PERSONNES CONCERNÉES	ÉVALUATION DU PRÉJUDICE SÉRIEUX	DATE DE L'AVIS À LA CAI	DATE DE L'AVIS AUX PERSONNES CONCERNÉES	DATE AVIS PUBLIC ET JUSTIFICATION	AUTRES INFORMATIONS

1.17 Avis aux personnes concernées concernant un incident de confidentialité

49

Par courrier recommandé

Ville et date

Madame (ou Monsieur) (nom)

(adresse)

Objet : Incident de confidentialité

Madame (ou Monsieur),

La présente vise à vous informer que, malheureusement, un incident de confidentialité vous concernant est survenu le (date).

En effet (description des informations visées, description des circonstances provoquant l'incident avec les dates ou la période concernée).

Nous vous informons que les renseignements personnels visés par le présent avis sont :

- XXXXXXXXXXX XXXX
- XXXXXXXXXXX XXXX
- XXXXXXX XXXXX
- XXXXXX XXXX

Nous prenons au sérieux cet incident et nous sommes actuellement à mettre en place toutes les mesures nécessaires pour diminuer les risques qu'un préjudice sérieux vous soit causé, entre autres nous avons pris et prenons toujours les mesures suivantes :

- XXXXXXXXXXX XXXX
- XXXXXXXXXXX XXXX

- XXXXXX XXXXX
- XXXXXX XXXX

Nous nous permettons de vous recommander de prendre les mesures suivantes afin de diminuer le risque qu'un préjudice sérieux vous soit causé :

- XXXXXXXXXXX XXXX
- XXXXXXXXXXX XXXX
- XXXXXX XXXXX
- XXXXXX XXXX

Pour toute information supplémentaire, je vous invite à communiquer avec moi.

Veuillez agréer, Madame (ou Monsieur), nos salutations distinguées.

XXX XXXXX

Le responsable de la protection
des renseignements personnels

1.18 Le temps de conservation des renseignements personnels

51

Documents	Durée de conservation
Documents en rapport à l'équité et le maintien de l'équité salariale	6 ans à compter de l'affichage des résultats
Documents fiscaux	7 ans ou demander la permission
Documents relatifs aux formations complétées	6 ans
Documents rattachés à un litige	3 ans
Dossiers de congédiement	3 ans
Registres de paie et documents relatifs	3 ans
Dossier médical du travailleur dans le cadre d'un programme de santé	Le Directeur de la santé publique doit s'assurer de la conservation du dossier médical d'un travailleur : 20 ans après la fin de son emploi ou 40 ans après le début de son emploi, selon la plus longue durée (nous suggérons la même durée)
Documents en lien avec le processus d'embauche (questionnaire de préembauche, examen médical, notes d'entrevues, tests de connaissance, etc.)	Le temps requis pour permettre au candidat non retenu d'épuiser l'ensemble des recours prévus dans la loi (incluant le recours en révision et d'appel), à compter de la date de la fin du processus d'embauche.
Procès-verbaux des réunions du Comité de santé et sécurité du travail	5 ans
Relevés d'emploi	6 ans
Documents qui font l'objet d'une demande d'accès ou de rectification	Aucun délai, cependant, lorsqu'un renseignement personnel fait l'objet d'une demande d'accès qui est refusée par l'entreprise, il faut le conserver le temps requis pour permettre à la personne concernée d'épuiser les recours prévus à la Loi.

1.19 Demande de retrancher, d'une liste nominative, des renseignements personnels

52

(Ville et date)

Monsieur Kevin Massé

Associé

(Coordonnées du responsable dans l'entreprise)

OBJET : Demande de retrancher d'une liste nominative des renseignements personnels

Madame, Monsieur,

En vertu de l'article 25 de la Loi sur la protection des renseignements personnels dans le secteur privé, je vous demande de retrancher les renseignements personnels me concernant de la liste nominative que vous détenez et utilisez. *(Expliquez brièvement la situation ou le contexte et précisez, s'il y a lieu, le nom de l'entreprise qui détient ou utilise cette liste).*

Vous en remerciant à l'avance, je vous prie d'agréer, Madame, Monsieur, mes salutations distinguées.

Signature :

Nom, prénom :

Adresse :

Tél. jour :

()

53