

Politique de confidentialité et de gestion des renseignements personnels

TABLE DES MATIERES

1. OBJECTIFS.....	2
2. RENSEIGNEMENTS PERSONNELS.....	3
3. COLLECTE.....	3
4. UTILISATION.....	3
5. CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS AU TRAVERS D'UN MOYEN TECHNOLOGIQUE.....	4
6. COMMUNICATION.....	6
7. CONSERVATION.....	7
8. DESTRUCTION.....	8
9. DEMANDE D'ACCÈS OU DE RECTIFICATION.....	8
10. INCIDENTS DE CONFIDENTIALITÉ.....	8
11. PROCESSUS DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.....	10
12. COORDONNÉES DE LA RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.....	10
ANNEXE 1 - PROCÉDURE DE NUMÉRISATION.....	11
ANNEXE 2 - REGISTRE DE NUMÉRISATION.....	12
ANNEXE 3 - TECHNIQUES DE DESTRUCTION DÉFINITIVE DE DOCUMENTS.....	13
ANNEXE 4 - REGISTRE DE DESTRUCTION.....	14
ANNEXE 5 - REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ.....	15
ANNEXE 6 - PROCÉDURE DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.....	16

1. OBJECTIFS

La présente Politique décrit les normes de collecte, d'utilisation, de communication et de conservation des renseignements personnels afin d'assurer la protection de ces renseignements.

2. RENSEIGNEMENTS PERSONNELS

Dans le cadre de ses activités, l'entreprise peut recueillir et traiter différents types de renseignements personnels, y compris :

- des renseignements d'identité, comme un nom ou un prénom, âge, date de naissance;
- des coordonnées de contact, une adresse, une adresse électronique et un numéro de téléphone;
- des renseignements relatifs aux dossiers des employés.;
- tout autre renseignement personnel nécessaire dans le cadre de ses activités.

3. COLLECTE

L'entreprise collecte des renseignements personnels auprès de sa clientèle et des employés.

De façon générale, l'entreprise collecte les renseignements personnels directement auprès de la personne concernée et avec son consentement, sauf si une exception est prévue par la loi.

Le consentement peut être obtenu de façon implicite dans certaines situations, par exemple, lorsque la clientèle décide de fournir volontairement ses renseignements personnels dans le cadre volontaire des activités de restauration, notamment pour les commandes pour emporter et la réservation de tables.

Dans tous les cas, l'entreprise ne collecte des renseignements personnels que s'il a une raison valable de le faire. De plus, la collecte ne sera limitée qu'aux renseignements nécessaires dont il a besoin pour remplir l'objectif visé.

À moins d'une exception prévue par la loi, l'entreprise demandera le consentement de la personne concernée avant de collecter des renseignements personnels qui la concernent auprès d'un tiers.

4. UTILISATION

L'entreprise s'engage à utiliser les renseignements personnels en sa possession uniquement aux fins pour lesquelles ils ont été recueillis et pour lesquels la loi l'autorise à les utiliser. Il peut toutefois les recueillir, les utiliser ou les divulguer sans le consentement de la personne visée lorsque cela est permis ou exigé par la loi.

Dans certaines circonstances particulières, l'entreprise peut recueillir, utiliser ou divulguer des renseignements personnels sans que la personne concernée soit en informée ou qu'elle n'ait donné son consentement. De telles circonstances sont réunies notamment lorsque, pour des raisons juridiques, médicales ou de sécurité, il est impossible ou peu probable d'obtenir son consentement, lorsque cette utilisation est manifestement au bénéfice de cette personne, lorsque cela est nécessaire pour prévenir ou détecter une fraude ou pour tous autres motifs sérieux.

L'entreprise limite l'accès des membres du personnel aux seuls renseignements personnels et connaissances de nature personnelle qui sont nécessaires à l'exercice de leur fonction.

5. CONFIDENTIALITÉ DES RENSEIGNEMENTS PERSONNELS AU TRAVERS D'UN MOYEN TECHNOLOGIQUE

L'entreprise s'engage à assurer la protection et la confidentialité des renseignements personnels recueillis sur le site Internet de l'entreprise ou par autres moyens technologiques.

Consentement

Lorsqu'un client utilise le site internet de l'entreprise ou des services technologiques et qu'elle soumette des renseignements personnels, ceux-ci sont réputés avoir donné leur consentement aux fins énoncées ci-après, pour lesquelles l'entreprise recueille et utilise vos renseignements personnels.

L'entreprise emploie la technologie des témoins de connexion pour aider les utilisateurs de son site Internet à naviguer plus rapidement et leur proposer le contenu qui les intéresse le plus.

Un témoin de connexion est une chaîne d'informations qui est envoyée par un site internet et stockée sur le disque dur ou temporairement dans la mémoire d'un ordinateur.

L'emploi des témoins de connexion se veut une pratique courante dans l'industrie et plusieurs fureteurs reconnus sont initialement configurés pour les accepter. Vous pouvez reconfigurer le vôtre afin qu'il refuse ou accepte les témoins de connexion ou encore qu'il vous alerte lorsqu'un témoin de connexion s'installe sur votre ordinateur. Notez qu'en refusant les témoins de connexion (cookies), vous pourriez ne pas être en mesure d'exploiter certaines fonctionnalités du site de l'entreprise.

Quel type d'information recueillons-nous?

La décision de nous fournir ou non vos renseignements personnels revient exclusivement au client. En règle générale, ils peuvent consulter le site internet de l'entreprise ou communiquer avec celle-ci sans avoir à fournir de renseignements personnels. Toutefois, dans certains cas, il sera nécessaire pour l'entreprise de recueillir vos renseignements personnels.

Lorsque vous visitez le site internet de l'entreprise, celle-ci peut notamment recueillir et utiliser les catégories de renseignements personnels suivants :

- **Identification** : le prénom et nom.
- **Coordonnées** : numéro de téléphone et adresse électronique.
- **Interactions** : lors d'une réservation de table, une prise de commande ou autre activités liés à la restauration.

- **Utilisation de notre site** : lorsque vous naviguez sur le site Internet de l'entreprise, celle-ci recueille automatiquement certains renseignements personnels sur les fichiers témoins de votre fureteur, notamment l'adresse IP, la langue de correspondance, la date et l'heure des visites ainsi que les pages consultées.

Utilisation des renseignements personnels colligée par notre site

Les renseignements personnels ne sont utilisés qu'aux fins indiquées au moment de la collecte, soit lorsque le client divulgue ses renseignements sur notre site Internet. Les renseignements personnels principalement pour :

- **Communiquer et tenir informés** : pour envoyer une confirmation de rendez-vous, pour répondre à une question posée, un commentaire ou une demande d'information, pour faire parvenir une infolettre si un consentement a été donné préalablement, etc.;
- **Personnaliser, améliorer ou faciliter l'expérience sur le site Internet** : par exemple, afin d'emmagasiner de l'information de sorte que vous n'ayez pas à la réinscrire à chaque visite subséquente;
- **Toute autre utilisation permise ou requise par les lois applicables.**

Partage et communication de l'information

L'entreprise ne peut transmettre des renseignements personnels à d'autres organisations qu'avec le consentement des personnes concernées. L'entreprise pourra communiquer des renseignements personnels sans consentement si la loi y oblige ou le permet, mais le cas échéant, seuls les renseignements qui sont exigés seront communiqués.

Stockage et sécurité

L'entreprise prend les moyens techniques raisonnables pour assurer un environnement sécuritaire et protéger les renseignements personnels, tels que : barrières coupe-feu, usage d'antivirus, gestion des accès, détection des intrusions, copie de sauvegarde régulière. Cependant, étant donné la nature même du réseau public qu'est l'internet, le client reconnaît et accepte que la sécurité des transmissions via internet ne puisse être garantie. En conséquence, l'entreprise ne peut garantir ni assumer aucune responsabilité pour toute violation de confidentialité, piratage, virus, perte ou altération des données transmises par Internet.

Conservation

L'entreprise utilise et conserve les renseignements personnels aussi longtemps que nécessaire afin de satisfaire les finalités pour lesquelles ils ont été recueillis, ou comme la loi le permet ou l'exige.

L'entreprise se réserve le droit de détenir, pour une durée raisonnable, certains renseignements personnels pour se conformer à la loi, prévenir la fraude, résoudre une réclamation ou certains autres problèmes s'y rattachant, coopérer à une enquête et pour tout autre acte permis par la loi. À l'expiration de ce délai, vos renseignements personnels seront délestés des serveurs de l'entreprise.

Liens externes

La présente Politique ne s'applique pas aux sites internet de tiers auxquels il est possible d'accéder en cliquant sur des liens qui se trouvent sur le présent site internet, et l'entreprise n'est nullement responsable à l'égard de tels sites internet de tiers. L'entreprise ne fait aucune représentation concernant tout autre site auquel vous pourriez avoir accès à partir du présent site. Lorsque le client accède un site Web de tiers, celui-ci disposera de ses propres politiques sur la protection des renseignements personnels que vous devrez examiner avant de soumettre des renseignements personnels.

Dans le cours de l'usage du site de l'entreprise, le client pourrait être amené à consulter d'autres sites web de tiers, via des hyperliens. Cependant, l'entreprise n'est pas responsable des pratiques, politiques ou actes de ces tiers en ce qui a trait à la protection de vos renseignements personnels.

De plus, un lien vers un tel site ne signifie pas que l'entreprise recommande ce site tiers ou qu'elle assume une quelconque responsabilité quant à son contenu ou à l'usage qui peut en être fait. Il incombe aux clients de prendre les précautions nécessaires pour assurer que le site sélectionné n'est pas infecté de virus.

Responsabilité

L'entreprise n'est pas responsable de l'exactitude des renseignements collectés sur son site Internet.

L'entreprise ne peut être tenu responsable de quelque dommage que ce soit causé de façon directe ou indirecte du fait de l'utilisation ou de la non-utilisation des informations diffusées sur le site.

L'entreprise ne garantit pas que le site ou son contenu ne seront pas l'objet d'interruptions ou d'erreurs, que les défauts éventuels seront corrigés, ni que le site ou le serveur qui l'héberge sont libres de virus ou d'autres éléments nuisibles.

Informations additionnelles

Pour toute demande d'information ou mise à jour concernant vos renseignements personnels, veuillez communiquer avec la Responsable de la protection des renseignements personnels par téléphone au _____ ou par courriel à l'adresse _____

Modification

L'entreprise se réserve le droit de modifier sa Politique de confidentialité à sa discrétion. L'entreprise rendra disponible, sur son site Internet, toute modification éventuelle de cette Politique de confidentialité.

6. COMMUNICATION

En principe, l'entreprise ne peut communiquer les renseignements personnels qu'il détient sur une personne sans le consentement de celle-ci.

Toutefois, l'entreprise peut communiquer à un tiers des renseignements personnels sans le consentement de la personne concernée lorsque la communication est due à une exigence réglementaire ou légale ou lorsque la *Loi sur le privé* ou toute autre loi le permet.

7. CONSERVATION

Conservation

Dans le cadre de ses activités, l'entreprise doit conserver de nombreux documents comportant des renseignements personnels, notamment pour les dossiers d'employés.

Certains documents doivent être conservés selon la durée prescrite par les lois en vigueur.

Qualité des renseignements personnels

L'entreprise s'assure de la qualité des renseignements personnels qu'il détient. En ce sens, les renseignements personnels conservés sont à jour, exacts et complets pour servir aux fins pour lesquelles ils ont été recueillis ou utilisés.

La mise à jour constante des renseignements personnels n'est pas nécessaire, sauf si cela est justifié par les fins pour lesquelles ce renseignement est recueilli. Cependant, si les renseignements doivent servir à une prise de décision, ils doivent être à jour au moment de celle-ci.

Documents physiques et numériques

Selon la nature des renseignements personnels, ceux-ci peuvent être conservés aux bureaux de l'entreprise, dans divers systèmes informatiques de l'entreprise ou de ses fournisseurs de services ou dans les installations d'entreposage de l'entreprise ou de ses fournisseurs de services

Mesures de sécurité

La sécurité et la protection des renseignements personnels sont importantes pour l'entreprise. Elle met en place des mesures de sécurité afin que les renseignements personnels demeurent strictement confidentiels et soient protégés contre la perte ou le vol et contre tout accès, communication, copie, utilisation ou modification non autorisée.

Ces mesures de sécurité peuvent notamment comprendre des mesures organisationnelles telles que la restriction des accès à ce qui est nécessaire; la sauvegarde et l'archivage des données au moyen d'un système externe, etc.); et mesures technologiques comme l'utilisation de mots de passe et de chiffrement (par exemple, le changement fréquent de mots de passe et l'utilisation de pare-feu).

(À conserver si l'entreprise va numériser les documents contenant des renseignements personnels)

Numérisation des documents

Dans l'éventualité où l'entreprise désire détruire les documents originaux à la suite de leur numérisation, il respecte les conditions suivantes :

1. L'information contenue dans les documents numérisés n'a pas été altérée et elle a été maintenue dans son intégralité ;
2. La numérisation ainsi que le support pour conserver les documents numérisés doit assurer la stabilité et la pérennité des documents.

L'entreprise choisit un support ou une technologie sur lequel il conserve ses documents qui lui permet de respecter ces conditions.

Lorsque l'entreprise effectue une numérisation de document, il applique la procédure prévue à l'**ANNEXE 1**. Elle consigne la numérisation dans le Registre de numérisation prévue à l'**ANNEXE 2**.

8. DESTRUCTION

La destruction des documents d'origine contenant des renseignements personnels ou confidentiels est faite de façon sécuritaire.

L'entreprise utilise des techniques de destruction définitive de documents adaptées au niveau de confidentialité du document à détruire.

Il se réfère à l'**ANNEXE 3** pour les techniques de destruction définitive de documents.

L'entreprise remplit le Registre de destruction prévu à l'**ANNEXE 4** lorsqu'il détruit des documents contenant des renseignements personnels.

9. DEMANDE D'ACCÈS OU DE RECTIFICATION

Toute personne peut faire une demande d'accès ou de rectification concernant les renseignements personnels détenus par l'entreprise.

La personne concernée doit soumettre une demande écrite à cet effet à la Responsable de la protection des renseignements personnels.

Sous réserve de certaines restrictions légales, les personnes concernées peuvent demander l'accès à leurs renseignements personnels détenus par l'entreprise et en demander leur correction dans le cas où ils sont inexacts, incomplets ou équivoques.

La Responsable de la protection des renseignements personnels doit répondre par écrit à ces demandes dans les 30 jours de la date de réception.

10. INCIDENTS DE CONFIDENTIALITÉ

Les incidents de confidentialité

Un incident de confidentialité correspond à un accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

L'entreprise, si elle a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient 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.

En cas d'incident de confidentialité, l'entreprise procède à l'évaluation du préjudice. Cette évaluation tient compte notamment des éléments suivants : la sensibilité des renseignements personnels concernés; les utilisations malveillantes possibles des renseignements et les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables.

Quand l'incident présente le risque qu'un préjudice sérieux soit causé aux personnes dont les renseignements sont concernés, l'entreprise avise par écrit :

- La Commission d'accès à l'information via le [formulaire d'avis](#) prescrit ;
- La ou les personnes concernées. L'avis doit permettre de la renseigner adéquatement sur la portée et les conséquences de l'incident.
 - Cet avis doit contenir :
 - Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'organisation doit communiquer la raison justifiant l'impossibilité de fournir cette description.
 - Une brève description des circonstances de l'incident;
 - La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue;
 - Une brève description des mesures prises ou envisagées pour diminuer les risques qu'un préjudice soit causé à la suite de l'incident;
 - Les mesures proposées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer celui-ci;
 - Les coordonnées d'une personne ou d'un service avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

Registre des incidents de confidentialité

L'entreprise tient un registre des incidents de confidentialité prévu à **l'ANNEXE 5**.

Le registre collige l'ensemble des incidents de confidentialité impliquant un renseignement personnel :

- ceux ne présentant pas de risque de préjudice sérieux et;
- ceux présentant un risque de préjudice sérieux.

Les renseignements contenus au registre des incidents de confidentialité sont tenus à jour et conservés pendant une période minimale de cinq (5) ans après la date ou la période au cours de laquelle l'entreprise a pris connaissance de l'incident.

11. PROCESSUS DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Toute personne concernée par l'application de la présente Politique peut porter plainte concernant l'application de la présente Politique ou, plus généralement, concernant la protection de ses renseignements personnels par l'entreprise.

La procédure de traitement de plainte relative à la protection des renseignements personnels est prévue à l'**ANNEXE 6**.

12. COORDONNÉES DE LA RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La Responsable de la protection des renseignements personnels peut être contactée par téléphone au _____ ou par courriel au _____

ANNEXE 1 – PROCÉDURE DE NUMÉRISATION

La personne responsable de la numérisation :

1. Effectue la préparation physique des documents à numériser (enlève les trombones et les agrafes);
2. Numérise les documents et demeure présente tout au long du processus afin de protéger l'intégrité des données numérisées;
3. Effectue une vérification exhaustive des documents numérisés afin de s'assurer de la quantité, de la qualité et de l'intégrité des documents reproduits. Elle vérifie que :
 - les documents numérisés sont conformes aux documents sources;
 - les données sont lisibles et de bonne qualité (sans perte de détail ou d'information);
 - le recto verso a bien été fait, le cas échéant; si l'option recto verso a fait en sorte de laisser des pages blanches, elle élimine ces dernières;
 - les documents ou les pages ont été numérisés dans le bon sens.
4. Vérifie que le nombre de documents ou de pages est exact (si des pages manquent, elle reprend la numérisation au complet);
5. Renomme les fichiers PDF selon la convention de nommage établie dans l'entreprise;
6. Enregistre le ou les fichiers PDF dans le logiciel approprié;
7. Consigne la numérisation dans le registre.

ANNEXE 2 – REGISTRE DE NUMÉRISATION

Registre de numérisation				
Date de numérisation	Description du ou des documents	Lieux enregistrement	Destruction du support papier (oui/non)	Numérisation fait par

ANNEXE 3 - TECHNIQUES DE DESTRUCTION DÉFINITIVE DE DOCUMENTS

Techniques de destruction définitive de documents¹

Support utilisé	Exemples de méthodes de destruction
Papier (original et toutes les copies)	<ul style="list-style-type: none">• Déchiqueteuse, de préférence à découpe transversale <p>Si les documents sont très confidentiels : déchiqueteuse + incinération</p>
Médias numériques que l'on souhaite réutiliser ou recycler Ex. cartes de mémoire flash (cartes SD, XD, etc.) clés USB, disque dur d'ordinateur	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Destruction physique (déchiquetage, broyage, meulage de surface, désintégration, trouage, incinération, etc.). <p>La plupart des déchiqueteuses pourront détruire les CD et les DVD.</p> <ul style="list-style-type: none">• Démagnétiseur pour les disques durs.
Machines contenant des disques durs Ex. photocopieur, télécopieur, numériseur, imprimante, etc.	<ul style="list-style-type: none">• Écrasement des informations sur le disque dur ou disque dur enlevé et détruit lorsque les machines sont remplacées.

¹ Commission d'accès à l'information, Procédure de destruction, en ligne :
<https://www.cai.gouv.qc.ca/entreprises/procedure-de-destruction/>

ANNEXE 5 - REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Registre des incidents de confidentialité								
Date ou période de l'incident	Personnes concernées (informations compromises)	Description des circonstances de l'incident	Prise de connaissance de l'incident	Nombres de personnes concernées par l'incident	Description des éléments qui amènent à conclure qu'il existe ou non un risque qu'un préjudice sérieux ² soit causé aux personnes concernées	Date de transmission de l'avis à la Commission d'accès à l'information	Date de transmission des avis aux personnes concernées	Description des mesures prises afin de diminuer les risques qu'un préjudice soit causé

² L'évaluation du risque de préjudice sérieux tient compte notamment des éléments suivants : la sensibilité des renseignements personnels concernés; les utilisations malveillantes possibles des renseignements et les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables.

ANNEXE 6 - PROCÉDURE DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Réception de la plainte

Toute personne qui souhaite formuler une plainte relative à l'application de la présente politique ou, plus généralement, à la protection de ses renseignements personnels par l'entreprise, doit le faire par écrit en s'adressant à la Responsable de la protection des renseignements personnels.

La personne devra indiquer son nom, ses coordonnées pour le joindre, incluant un numéro de téléphone, ainsi que l'objet et les motifs de sa plainte, en donnant suffisamment de détails pour que celle-ci puisse être évaluée par l'entreprise. Si la plainte formulée n'est pas suffisamment précise, le responsable de la protection des renseignements personnels peut requérir toute information additionnelle qu'il juge nécessaire pour pouvoir évaluer la plainte.

Traitement de la plainte

L'entreprise s'engage à traiter toute plainte reçue de façon confidentielle.

La plainte est traitée dans un délai raisonnable. La Responsable de la protection des renseignements personnels doit évaluer la plainte et formuler une réponse motivée écrite à la personne plaignante.

Cette évaluation visera à déterminer si le traitement des renseignements personnels par l'entreprise est conforme à la présente politique et pratique en place au sein de l'organisation et à la législation ou réglementation applicable.

Dossier de plainte

L'entreprise doit constituer un dossier distinct pour chacune des plaintes qui lui sont adressées en vertu de la présente procédure de traitement de plainte. Chaque dossier contient la plainte, l'analyse et la documentation à l'appui de son évaluation, ainsi que la réponse écrite envoyée à la personne plaignante.